DOI https://doi.org/10.36059/978-966-397-374-6-28

ПРОБЛЕМНІ ПИТАННЯ ЗАКОНОДАВЧОГО ВРЕГУЛЮВАННЯ ПОНЯТТЯ БОТОФЕРМ

Дрижакова Д. Ю.
аспірантка кафедри кримінально-правової політики
та кримінального права
Київського національного університету імені Тараса Шевченка
м. Київ, Україна

Стаття присвячена проблемам вдосконалення правового забезпечення охорони безпеки електронних комунікаційних систем, електронних мереж та комп'ютерних даних, як частини інформаційної безпеки.

Питання кібезлочинності та ботоферм перетворюються на всесвітні проблеми, регулюванню яких приділяють значну увагу сучасні дослідники на національному та міжнародному рівнях.

З 24-го лютого 2022 року особливу увагу почали приділяти відносно новому елементу кіберзлочинності – ботофермам. Завдання угрупувань ботів полягає у підбурюванні до зміни територіальної цілісності та незалежності України, у поширенні фейкової інформації щодо ситуації на прифронтових та окупованих територіях та у наданні неправдивої інформації про представників державної влади з метою налаштування населення проти влади. Таким чином, сьогодні інструменти кіберзлочинності займають особливу роль в інформа– ційній боротьбі українського народу, тому регулювання цих питань в правовій системі України посідає важливе місце.

Метою статті є аналіз шляхів вирішення проблеми «ботоферм».

Ключові слова: несанкціоноване втручання, ботоферми, законодавча неврегулюваність, кібепростір, кібертероризм.

Виклад основного матеріалу. З початку війни Україна зазнала численних кібератак. У нещодавньому звіті Держспецзв'язку України йдеться про те, що хакери отримали доступ до комп'ютерних систем, відкривши «No. 1275» повідомлення електронної пошти. Цей електронний лист містив вкладення, яке давало хакерам повний контроль над зараженою системою. Під час воєнного стану кіберзлочинці можуть атакувати інформаційну оборону України, використовуючи інформаційні простори, не покладаючись на ворога, який використовує це для заподіяння шкоди суверенітету країни. Вони також можуть використовувати переобтяжені правоохоронні органи та викрадати кошти у громадян з використанням мережі Internet.

З початку військової агресії РФ рівень кіберзлочинності в Україні стабільно зростав. Слід зазначити, що інформаційна війна може завдати стільки ж шкоди, скільки й реальні бойові дії на полі бою [1].

З початку 2022 р. Служба безпеки України нейтралізувала понад 4,5 тис. кібератак на Україну. Якщо у 2020 р. було зафіксовано майже 800 кібератак, у 2021 – 1400, то вже минулого року їхня кількість зросла більш як утричі [2].

Наведені дані свідчать про ведення проти України так званої кібервійни. Разом з тим у законодавстві України поняття кібервійни не закріплене. Законом України «Про основні засади забезпечення кібербезпеки України» надаються дефініції таких понять як кібербезпека, кіберзлочин та ін. Так, під кіберзлочином (комп'ютерним злочином), згідно п. 8 ч. 1 цього Закону, законодавець розуміє суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнане злочином міжнародними договорами України [3].

Окрему увагу слід приділити ботофермам. На сьо– годні їх існує чотири основні типи – соціальні боти в електронній комерції, SEO-боти (репостери неправдивої інформації), боти-багатоденники та політичні боти. Під час повномасштабного вторгнення особливу увагу слід приділяти саме останньому виду ботів, які в своїй сукупності утворюють «ферму». Роль політичних ботів полягає в поширенні неправдивої інформації через соціальні мережі за рахунок спілкування між людьми. Тобто особливістю цього виду ботів є їх підключення до мережі спілкування, вони можуть односкладово відповідати на будь-які повідомлення.

Таким чином, метою діяльності проросійських бото-ферм залишається дискредитація міжнародного іміджу України та усієї системи державної влади України.На постійній основі фіксується неабиякий бурхливий сплеск активності проросійських ботоферм у соціальних мережах [4].

Україна перебуває у переліку країн, де з 2017 року виявили найбільшу кількість ботоферм у соціальних мережах, а у військовий час ця кількість значно зростає.

На жаль, законодавство не встигає такими темпами освоювати нові правопорушення.

У вересні 2023 року СБУ звітувало, що знешкодило біля 80 бото-ферм, а дії з їх створення класифікуються за статтею 361 Кримінального кодексу України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», ст. 111 КК України – державна зрада, ст. 110 КК України – посягання на

територіальну цілісність України, ст.109 КК України – публічні заклики до повалення конституційного ладу.

На ефективність заходів із протидії використанню «ботоферм» на шкоду національній безпеці України негативно впливає законодавча неврегульованість використання подібних апаратно-програмних комплексів.

Група народних депутатів 19 квітня 2023 року зареєструвала законопроєкт № 9223 «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо встановлення відповідальності за окремі дії проти основ національної безпеки України». Законопроєкт пропонує доповнити Кримінальний кодекс України статтею 114-3 «Використання облікових записів з метою поширення недостовірної інформації або для здійснення впливу на прийняття рішень, вчинення чи невчинення дій».

Зокрема, за створення, придбання, використання або збут облікових записів в інформаційних (автоматизованих), електронних комунікаційних, інформаційних системах, електронних комунікаційних мережах – тобто у соціальних мережах типу Facebook, Instagram, Twitter тощо – загрожує покарання від штрафу до позбавлення чи обмеження волі.

Однак не всі зазначені дії будуть каратися. Згідно з проєктом закону, до ознак складу злочину належать такі:

Облікові записи містять завідомо неправдиві відомості щодо користувача.

За допомогою облікового запису здійснюється розміщення та поширення недостовірної інформації (у тому числі від імені інших осіб, причетність яких до оприлюдненої інформації не підтверджена) або втручання в діяльність фізичних і юридичних осіб.

Дії вчинені на шкоду суверенітету, територіальній цілісності та недоторканості, обороноздатності, національній, державній, економічній чи інформаційній безпеці України.

За відсутності ознак державної зради порушникам загрожує штраф у розмірі від однієї до трьох тисяч неоподатковуваних мінімумів доходів громадян, тобто 17-51 тис. грн або виправні роботи строком до двох років. При здійсненні цих дій повторно чи групою осіб за попередньою змовою або для впливу на державні чи місцеві органи, їхніх посадових осіб, зловмисникам загрожує обмеження чи позбавлення волі на строк від трьох до п’яти років. Ще більший строк, до семи років із конфіскацією майна, загрожує у випадку скоєння злочину в умовах воєнного стану.

Якщо ж використання облікових записів сприяє підвищенню рівня соціальної напруги, порушують конституційні права і свободи громадян, або іншим чином загрожують національній безпеці, однак немає ознак державної зради, то передбачається штраф у розмірі від семисот

п’ятдесяти до тисячі неоподатковуваних мінімумів доходів громадян (12,75 – 17 тис. грн) або виправні роботи до одного року.

Такі зміни, на думку авторів законопроєкту, покликані захистити національні інтереси в інформаційній сфері, зважаючи на активне «використання ботів у соціально орієнтованих ресурсах мережі Інтернет для здійснення деструктивної інформаційної діяльності», мовиться у пояснювальній записці.

Крім того, законопроєкт пропонує віднести досудове розслідування цього злочину до компетенції Служби безпеки України.

Висновки: Україна активно долучає свою частку зусиль до міжнародної боротьби з пропагандою та фейками. На цьому фоні потребує активізації діяльність, спрямована на нейтралізацію впливу дезінформації та маніпуляцій, впровадження швидкого та проактивного реагування на ключові теми, у межах яких поширюють фейки та пропаганду. Тому в сучасних умовах доцільним є внесення змін до законодавства про удосконалення кримінальної відповідальності за поширення фейкової інформації та дезінформації. Приведення законодавства у відповідність європейських стандартів.

Література:

1. Кількість кібератак на Україну продовжує зростати. Держспецзв’язк. Економічна правда: веб-сайт. URL:https://www.epravda.com. ua/news/2022/11/10/693694/

2. Кібервійна рф проти України: як працюють російські хакери та воюють українські кібервійська. URL: https://thepage.ua/ua/politics/ kibervijna-rf-proti-ukrayini-yak-voyuyut-ukrayinski– kibervijska

3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Tex

4. Кіца М.О. Фейкова інформація в українських соціальних медіа: поняття, види, вплив на аудиторію. URL: http://nz.uad.lviv.ua/static/ media/1–52/36

5. В Україні ліквідували «мільйонну ботоферму»: що це за боти і до чого тут Порошенко? Радіо свобода. URL: https://www. radiosvoboda.org/a/botoferma-sbu-poroshenko/31972104.html

6. Юшков А.Г. Загрозливі тенденції використання ботоферм на шкоду державним інтересамУкраїни: Механізми запобігання та протидії. Інформація і Право. 2021. No 3(38) С. 90-98.

7. «Законодавчий спам» проти «ботоферм»: неепічна битва // https://lb.ua/blog/voxukraine/554011_zakonodavchiy_spam_proti.html