УДК 343.9
DOI https://doi.org/10.32782/2408-9257-2024-1-48

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

# ПРОБЛЕМНІ ПИТАННЯ ЗАКОНОДАВЧОГО ВРЕГУЛЮВАННЯ ПОНЯТТЯ БОТОФЕРМ

# PROBLEMATIC ISSUES OF LEGISLATIVE REGULATION OF THE CONCEPT OF BOTANICAL FARMS

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.

Ботоферми, або так звані «ферми ботів», є сферою зростаючого інтересу у зв'язку зі зростанням використання ботнетів для злочинних цілей, таких як кібератаки, крадіжка даних, шахрайство і т. ін.

У статті розглядаються питання, пов'язані з юридичними аспектами функціонування ботоферм, включаючи їх визначення, види злочинів, пов'язаних з ними, а також відповідальність за їх створення, управління та використання. Аналізується діюче законодавство, яке регулює цю сферу, і висуваються пропозиції щодо його вдосконалення з метою забезпечення більшої ефективності у протидії кіберзлочинності. Робота важлива для розуміння правових аспектів боротьби з ботофермами та розвитку відповідних правових механізмів у цій сфері.

В статті висвітлюються проблемні питання пов'язані з ботофермами у контексті кібербезпеки, а саме з приводу того, що злочинці можуть використовувати ботоферми для зловживання обчислювальними ресурсами для проведення масштабних кібератак, включаючи DDoS-атаки, фішингові кампанії та інші злочинні дії; ботоферми можуть бути використані для розповсюдження шкідливих програм, таких як віруси, троянці та різноманітні види шпигунського програмного забезпечення; шляхом зараження комп'ютерів у ботофермі може бути вкрадена конфіденційна інформація, така як особисті дані користувачів, фінансова інформація та інші чутливі дані; ботоферми можуть бути використані для проведення різноманітних фінансових шахрайств, таких як фішингові атаки, шахрайство з кредитними картками та інші види кібершахрайств.

***Ключові слова:*** *несанкціоноване втручання, ботоферми, законодавча неврегульованість, кібепростір, кібертероризм.*

The article is devoted to the problems of improving the legal support for the security of electronic communication systems, electronic networks and computer data as part of information security.

The issues of cybercrime and bot farms are turning into global problems, the regulation of which is receiving considerable attention from modern researchers at the national and international levels.

Bot farms, or the so-called "bot farms", are an area of growing interest due to the increasing use of botnets for criminal purposes, such as cyberattacks, data theft, fraud, etc.

The article addresses issues related to the legal aspects of bot farms, including their definition, types of crimes related to them, and liability for their creation, management and use. The current legislation governing this area is analyzed and proposals for its improvement are put forward in order to ensure greater effectiveness in combating cybercrime. The work is important for understanding the legal aspects of combating bot farms and developing appropriate legal mechanisms in this area.

The article highlights the problematic issues related to bot farms in the context of cybersecurity, namely that criminals can use bot farms to abuse computing resources to conduct large-scale cyberattacks, including DDoS attacks, phishing campaigns and other criminal activities; bot farms can be used to spread malicious programs such as viruses, trojans and various types of spyware; confidential information, such as personal data of users, financial information and other sensitive data, can be stolen by infecting computers in a bot farm; bot farms can be used to conduct various financial frauds, such as phishing attacks, credit card fraud and other types of cyber fraud.

***Key words:*** *unauthorized interference, bot farms, legislative unregulation, cyberspace, cyberterrorism.*

**Актуальність теми дослідження.** 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 інформаційній боротьбі українського народу, тому регулювання цих питань в правовій системі України посідає важливе місце.

Питання безпеки віртуального простору стає все більш актуальним у зв'язку з зростанням використання ботнетів для кібератак і злочинних дій в Інтернеті. Ботоферми або «ферми ботів» можуть бути використані для створення та управління ботнетами, що можуть бути використані для різних злочинних цілей.

Саме тому, вважаю, варто приділити увагу діяльності ботоферм, їх законному врегулюванні та більш детально дослідити принцип їх функціонування, задля вчасного забезпечення недопущення несанкціонованого втручання у ці системи.

**Аналіз досліджень і публікацій з проблеми.** Питання законодавчого врегулювання поняття ботоферм станом на зараз є майже недослідженим. Зокрема, з науковців можливо виділити лише Юшкова А.Г., який присвятив свої праці дослідженню даного питання. Інші ж науковці, здебільшого лише в загальному розумінні досліджували питання законодавчого врегулювання ботофер, без виокремлення кібератак, несанкціонованого втручання та, безпосередньо, ботоферм.

**Метою статті** є аналіз шляхів вирішення проблеми «ботоферм», зокрема можливість врегулювання законодавчо, адже задля боротьби з цією небезпекою необхідно розвивати технології кібербезпеки, вдосконалювати алгоритми виявлення та блокування атак, а також співпрацювати на міжнародному рівні для обміну інформацією та координації дій проти кіберзлочинності.

**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.

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.

Сам термін «бот» (скорочення від «робот») з'явився саме з появою в інтернеті соціальних мереж. Коли люди масово почали створювати свій віртуальний образ для спілкування в анонімному світі комунікацій, з'явились вони – інтернет-боти, деперсоналізовані акаунти. Практично кожен активний користувач соціальних мереж мав своє «альтер его» на випадок, що його заблокують. Або якщо думки, які він хоче донести, ідуть в розріз з масовою думкою його аудиторії, то вкинути їх можна з акаунту людини, якої не існує…

Ботоферма – це система, яка автоматизовано керує множинними обліковими записами (ботами) в соціальних мережах, на форумах,

веб-сайтах та інших онлайн-платформах. Ці боти можуть бути запрограмовані на виконання різних завдань, таких як:

• Розповсюдження інформації: боти можуть публікувати пости, коментарі та ретвіти, щоб поширити певну інформацію або ідею.

• Маніпулювання громадською думкою: боти можуть використовуватися для створення ілюзії підтримки або незгоди з певною темою.

• Спам: боти можуть розсилати спам-повідомлення, щоб рекламувати продукти або послуги.

• Атаки на веб-сайти: боти можуть використовуватися для DDoS-атак, щоб перевантажити веб-сайт та зробити його недоступним.

Значення ботоферм у сучасному світі:

• Політика: ботоферми можуть використовуватися для впливу на результати виборів, поширення дезінформації та пропаганди.

• Бізнес: ботоферми можуть використовуватися для просування продуктів і послуг, а також для створення фейкових відгуків.

• Соціальні мережі: ботоферми можуть використовуватися для накручування лайків, підписників та переглядів.

Негативні наслідки використання ботоферм:

• Поширення дезінформації: ботоферми можуть використовуватися для поширення фейкових новин та пропаганди.

• Маніпулювання громадською думкою: ботоферми можуть використовуватися для створення ілюзії підтримки або незгоди з певною темою.

• Спам: ботоферми можуть розсилати спам-повідомлення, які можуть бути annoying and even harmful.

• Атаки на веб-сайти: ботоферми можуть використовуватися для DDoS-атак, які можуть призвести до значних фінансових втрат.

На сьогодні існує чотири основні типи ботоферм – соціальні боти в електронній комерції, SEO-боти (репостери неправдивої інформації), боти-багатоденники та політичні боти [4]. 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.

Основні технології, що використовуються в ботофермах:

• Програмне забезпечення для автоматизації: використовується для автоматизації завдань, таких як створення ботів, публікація повідомлень,

• Програмне забезпечення для керування ботами: використовується для керування ботами.

• Програмне забезпечення для збору даних: використовується для збору даних про користувачів.

• Програмне забезпечення для аналізу даних: використовується для аналізу даних.

• Проксі-сервери: використовуються для приховування IP-адрес ботів.

• Сервіси CAPTCHA: використовуються для відрізнення ботів від людей.

МАЙДАНЧИКАМИ ДЛЯ БОТОФЕРМ МОЖУТЬ БУТИ:

1. Соцмережі. Фоловери у соцмережах, лайки та коментарі – це величезний ринок, де щорічно люди витрачають шести- та семизначні суми на придбання кліків ботів. Боти лайкають облікові записи та підписуються на них, аби підвищити довіру до певних облікових записів, брендів, бізнесу та зробити їх популярнішими.

2. Twitch/YouTube потоки. Прибуток блогерів залежить від кількості переглядів, які збирає їхній контент. Звичайно, блогери купують трафік-ботів, щоб збільшити кількість переглядів та залучити більше рекламодавців. Ця накрутка відома як накрутка за допомогою «переглядових ботів».

3. Рекламні банери. Кліки PPC – натискання на рекламу з оплатою принесе рекламній платформі більше грошей. Шахрайські кліки у деяких кампаніях PPC сягають 60%.

4. Сайти. Вебмайстри можуть купувати трафік-ботів, щоб збільшити відвідуваність сайту та отримувати більше грошей за рекламу. Вони також можуть монетизувати кліки у інший спосіб. Наприклад, стягуючи плату за «якісні зворотні посилання».

Таким чином, метою діяльності проросійських ботоферм залишається дискредитація міжнародного іміджу України та усієї

системи державної влади України.На постійній основі фіксується неабиякий бурхливий сплеск активності проросійських ботоферм у соціальних мережах [5, с. 90–98].

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

СБУ ліквідувала значну кількість ворожих ботоферм за період повномасштабного вторгнення потужністю понад 100 тисяч фейкових акаунтів. За завданням спецслужб РФ, інтернет-агенти проводили масштабні інформаційні диверсії для розхитування внутрішньої обстановки в країні та сприяння окупантам.

Ботоферми були зосереджені на території Харкова, Черкас, Тернополя і Закарпатської області. Для підривної роботи використовували соцмережі, у тому числі заблоковані провайдерами в Україні.

Боти поширювали дезінформацію щодо повномасштабного російського вторгнення в Україну та розповсюджували фейкові «новини з фронту».

Так, у ході операції «Ботоферма» було припинено діяльність 13 ботоферм, які налічували понад 1,5 мільйона фейкових акаунтів у різних соціальних мережах, поштових сервісах та месенджерах.

Фігуранти операції «Ботоферма» використовували понад 100 тисяч SIM-карток, які реєструвалися на різних мобільних операторах, включаючи російських операторів. За допомогою цих SIM-карток фігуранти реєстрували фейкові акаунти в соціальних мережах, поштових сервісах та месенджерах.

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

На сьогодні відповідальність за таку діяльність – кримінальна, за різними статтями: від несанкціонованого втручання в роботу електронних мереж до пропаганди війни.

У вересні 2023 року СБУ звітувало, що знешкодило біля 80 ботоферм, 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 [6].

В СБУ вважають, що відповідальність за такий злочин має бути посилена, адже на сьогоднішній день створення ботоферми класифікується, як несанкціоноване втручання у роботу електронно-обчислювальних мереж (ст. 361 Кримінального кодексу України) і карається штрафом або ж позбавленням волі від 2 до 6 років максимум.

Водночас чимало ботоферм працюють на російські спецслужби, а отже кваліфікувати такі дії вже варто, як пособництво державі-агресору чи й державну зраду, що тягне за собою значно вищий рівень відповідальності.

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» [7].

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. Держ спецзв'язок. Економічна правда URL: https://www.epravda.com.ua/news/2022/11/10/693694/ (дата звернення: 14.04.2024).

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 (дата звернення: 14.04.2024).

3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.04.2024).

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

5. Кіца М.О. Фейкова інформація в українських соціальних медіа: поняття, види, вплив на аудиторію. URL: file:///C:/Users/%D0%9F%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C/Downloads/Nz_2016_1_37.pdf (дата звернення: 14.04.2024).

6. 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 (дата звернення: 14.04.2024).

7. «Законодавчий спам» проти «ботоферм»: неепічна битва. URL: https://lb.ua/blog/voxukraine/554011_zakonodavchiy_spam_proti.html (дата звернення: 14.04.2024).