УДК 343.34
DOI https://doi.org/10.32782/2524-0374/2022-11/138

БОТОФЕРМИ ТА ІНШІ КІБЕРЗАГРОЗИ ПІД ЧАС ВОЄННОГО СТАНУ: ПИТАННЯ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ

BOT FARMS AND OTHER KIBEZAGROS DURING MARTIAL LAW: ISSUES OF CRIMINAL RESPONSIBILITY

Лисько Т.Д., к.ю.н.,
доцент кафедри кримінального права та процесу
Національний авіаційний університет
Паламарчук В.О., здобувачка вищої освіти першого (бакалаврського) рівня
Національний авіаційний університет

Дана наукова стаття присвячена актуальним проблемам кіберзлочинності, з якими зіткнулося людство останніми десятиліттями. Питання кібезлочинності та ботоферм перетворюються на всесвітні проблеми, регулюванню яких приділяють значну увагу сучасні дослідники на національному та міжнародному рівнях.

В епоху модернізації гаджетів та глобалізації процесу цифровізації, будь-яка людина без ниших намірів може стати злочинцем. Наприклад, завдяки інформаційній революції студент-інформатик з ноутбуком може вчиняти крадіжки з використанням мережі Internet. Значна частина населення використовує мобільні пристрої для спілкування та створення нових суспільних відносин.

Офіційне управління кримінальної статистики України повідомляє про зростання кіберзлочинів у 7,5 раза за останні 8 років. Це не враховуючи так звані «традиційні» комп'ютерні кримінальні правопорушення. Особливо небезпечними стали кіберзлочини під час дії правового режиму воєнного стану, адже кіберзлочинець перетворюється на спеціалізований бойовий підрозділ, який має свої завдання та механізми їх реалізації з використанням сучасних комп'ютерних технологій. Їх основними інструментами є хакерство та кібератаки. Кібератаки є особливим елементом інформаційної війни сьогодення. Кібератаки на інформаційні ресурси та на офіційні веб-сторінки представників української влади та органів управління – це суттєве погіршення становища ІТ-інфраструктури нашої держави.

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.

Ключові слова: інформаційна війна, хакерство, кіберзлочинність, ботоферма.

This scientific article is devoted to the current problems of cybercrime that humanity has faced in recent decades. The issues of cybercrime and bot farms are turning into global problems, the regulation of which is paying considerable attention to participants in international legal relations.

Living in the era of modernization of gadgets and globalization of the digitalization process, a person without cold-blooded intentions can be a thief. For example, thanks to the information revolution, a computer science student with a laptop may commit theft. The general public also uses mobile devices to communicate and create new social relationships.

The official Office of Criminal Statistics of Ukraine reports a 7.5-fold increase in cybercrimes over the past 8 years. That's not taking into account traditional computer crimes or the time it takes for cybercriminals to commit their crimes. During the war, the cybercriminal turns into a specialized combat unit. Their main tools are hacking and cyber attacks. Cyber attacks is a special element of today's information war. Cyber attacks on information resources and on the official web pages of Ukrainian representatives of the authorities and management bodies are a significant deterioration of the situation of the IT infrastructure of our country.

From February 24, special attention began to be paid to a relatively new element of cybercrime - bot farms. The role of the bot group is to incite the territorial integrity and independence of Ukraine, to spread fake information about the situation in the frontline and in the occupied territories, and to present false information about members of the state administration, in order to set the population against the authorities. Thus, today the tools of cybercrime have a special role in the information struggle of the Ukrainian people, therefore the regulation of these issues has an important place in the legal system of Ukraine.

Key words: information war, hacking, cybercrime, bot farm.

Постановка проблеми. Інформаційна війна за рахунок маніпулювання свідомістю громадян, керування напругою в країні та поширенням неправдивої інформації є одним із складових елементів порушення основ національної безпеки України, створює загрозу порушення її територіальної цілісності та суверенітету. На сьогодні ми спостерігаємо використання інформаційними кураторами Російської Федерації новітніх технологій: мікроблогів, соціальних мереж, ботоферм з аудиторією тощо, з метою здійснення протиправної діяльності проти нашої держави та заподіяння шкоди державним інтересам. За таких умов соціальні мережі в Україні залишаються найбільш вразливими з точки зору можливостей оприлюднення інформації антиукраїнського змісту та проведення інформаційних кампаній та акцій на шкоду інтересам держави. Останнім часом має прояв загрозлива тенденція використання ботоферм на шкоду державним інтересам України. Переважне використання ботоферм здійснюється через фейкові акаунти, де поширюється деструктивна інформація, з метою створення панічних настроїв населення.

Аналіз останніх досліджень та публікацій. Проблеми кіберзлочинності в цілому активно досліджується в працях як зарубіжних, так і вітчизняних науковців. Слід зауважити, що більшість науковців приділяють увагу психологічному аспекту, тобто реагуванню населення на кіберзлочин, та правовому аспекту, зокрема удосконаленню нормативно-правової бази регулювання даних суспільних відносин. Серед дослідників, які займалися вивченням даного питання, є Кіца М., Курбан О., Пригорницька О. Ткачук Н., Зінченко О., Юшков А. та інші.

Метою і завданням наукової статті є дослідження загроз національній безпеці зі сторони кіберзлочинності в Україні під час повномасштабного вторгнення, приділяючи особливу увагу значенню та ролі ботоферм.

Виклад основного матеріалу. Сьогодні трохи більше як чверть українців основним джерелом новин для себе вважають соціальні мережі. Новітньою тенденцією останніх років в кіберзлочинності стало застосування ботоферм. Як зазначає Юшков А.Г., «ботоферми – це компанії, які

масово створюють несправжніх користувачів соцмереж і від їхнього імені пишуть тисячі коментарів» [1, с. 92-93].

Ще одна спільна мета кіберзлочинів – зруйнувати інфраструктуру країни, включно з військовою та політичною системами. 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 [2].

Отже, відкрите вторгнення РФ в кіберпростір викликало потребу в покращенні заходів безпеки та захисту. Це призвело до змін чинного законодавства та захисту в частині цифрових технологій. Два з цих нових законів зосереджені на кримінальному провадженні: 1) Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» № 2137-IX від 15.03.2022 [3] та Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24.03.2022 [4].

Перш ніж аналізувати закони, слід приділити увагу термінології, пов'язаної з кіберзлочинністю. Український законодавець надав визначення кіберзлочинності. Кіберзлочин визначається як будь-яка злочинна дія, вчинена в Інтернеті або за допомогою нього. У Кримінальному кодексі України (далі – КК України) встановлена відповідальність за кіберзлочинність, яка є частиною міжнародних договорів, укладених та ратифікованих Україною.

Деградація інформаційних систем і мереж країни під час війни є частиною загальної мети кіберзлочинності. Це може бути зроблено для викрадення інформації або знищення систем даних і мереж. Шкідливе вкладення було розроблено, щоб дозволити хакерам викрасти конфіденційні дані та погрожувати втратою апаратного забезпечення, якщо заражений користувач не заплатить викуп. Згодом цей вектор атаки було використано як частину невдалої спроби підтримати фізичне вторгнення Росії в Україну.

Хакерська група Strontium мала намір використовувати цю підтримку для доступу до комп'ютерних систем в Україні, США та країнах Європейського Союзу, щоб забезпечити тактичну підтримку вторгнення Росії та викрасти конфіденційну інформацію. 4 квітня 2022 року Державна інформаційна служба оприлюднила звіт про фальшиву електронну пошту, яка свідчить про те, що російські військові злочинці обмінювалися інформацією. Відкриття фіктивної електронної пошти призводить до підробленого документа, який надає віддалений доступ до комп'ютера жертви [5].

Хакери також намагаються отримати доступ і контролювати існуючі системи та обладнання компанії. 28 березня 2022 року український провайдер «Укртелеком» зазнав потужної атаки. Під час цього заходу хакери намагалися проаналізувати IT-інфраструктуру компанії, відключити їхні служби та зібрати розвідувальні дані про мережу організації. Шкідлива програма під назвою Cobalt Strike Beacon була використана для зараження комп'ютерів під час відкриття. Це було зроблено 23 березня 2022 року ворогом з метою пошкодити державні установи України шляхом кібератаки. Вказані випадки невеликих хакерських атак і менших атак зазвичай не привертають уваги преси [6]. Це пов'язано з тим, що вони становлять лише невеликий відсоток усіх випадків.

Зміни, що були внесені у КК України, торкнулися двох норм глави XVI Особливої частини КК України. Вони набули чинності після прийняття Закону 2149-IX від 24.03.2022, який мав на меті забезпечення вищої спроможності та ефективності національної системи кібербезпеки у протидії кіберзагрозам. Наразі можемо констатувати, що необхідно докласти зусиль для створення кримінально-правових норм, які зможуть ефективно боротися з кіберзлочинністю. Так, ст. 361 КК України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» отримала нову редакцію.

Гарантування надійності і безпеки цифрових послуг – за цим явищем стоїть зміна термінології. Закон України «Про електронні комунікації» передбачає заміну таких термінів, як комп'ютери, автоматизовані системи, комп'ютерні мережі та телекомунікаційні мережі на «інформація, автоматизовані системи, електронний зв'язок та системи зв'язку». Це робиться відповідно до інших законів України, що стосуються кібербезпеки.

Окрім змін у термінології, ст. 361 ККУ також змінила визначення кримінальних протиправних дій, додавши до визначення об'єктивної сторони складу кримінального правопорушення несанкціоноване втручання.

Апарат ВРУ зазначає, що діяння, не становить істотної суспільної небезпеки, якщо воно не має наслідків. На нашу думку, слід зазначити, що це формулювання відповідає поточним обставинам, оскільки несанкціоноване втручання вже передбачає високий рівень загрози. А будь-які непередбачені наслідки можуть не реалізуватися чи не проявитися з причин, які не залежать від волі винного. Крім того, такий підхід спрощує судове провадження, оскільки звужує предмет доказування у кримінальному провадженні [7].

Стаття 361 КК України вказує, що під час воєнного стану підвищений ступінь суспільної небезпечності отримують лише окремі частини закону – ч. 3 та ч. 4 ст. 361 КК України, які встановлюють відповідальність за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації (ч. 3 ст. 361 КК України) та якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків (ч. 4 ст. 361 КК України) під час дії воєнного стану (ч. 5 ст. 361 КК України). Такі діяння тягнуть досить серйозну кримінальну відповідальність – позбавлення волі на строк від десяти до п'ятнадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Закон передбачає, що програмне або апаратне забезпечення, яке незаконно використовується, розповсюджується або продається, має бути створено. Крім того, розповсюдження або продаж шкідливого програмного чи апаратного забезпечення є незаконним. Розповсюдження чи продаж цих предметів є порушенням закону.

Україні потрібно було оновити свої закони, щоб дозволити їм виконувати програми Bug Bounty або запрошувати зовнішніх розробників для пошуку вразливостей у програмному забезпеченні, веб-сайтах і системах зв'язку. Хоча

можна констатувати, що на сьогодні правове регулювання сфери кібербезпеки в Україні ще не до кінця завершене.

Через триваючу війну в Україні виник неофіційний громадський рух під назвою «Кіберармія». Цей спонтанний рух опору використовує методи онлайн-війни, щоб завдати шкоди комп'ютерним системам противника та зірвати їхні плани [9]. Це також стосується як IT-фахівців, так і звичайних громадян. Навряд чи буде притягнуто до кримінальної відповідальності осіб, які вчиняють суспільно нешкідливі дії.

Оскільки кіберзлочини та хакерство під час війни зазвичай не вважаються пріоритетними, однак вважаємо, що цей новий закон є вкрай необхідним на сучасному етапі. КК України розширив відповідальність за кіберзлочини. Додаткова криміналізація окремих дій сприяє запобіганню кримінальних правопорушень у майбутньому. Через нинішні воєнні обставини взяти на себе відповідальність за кримінальні правопорушення, скоєні в кіберпросторі чи Україні, є виправданим. Запровадження цих суворих санкцій з боку держави є необхідним, тому що кожен, хто завдає шкоди національним інтересам країни, винен так само, як і військові злочинці.

Будь-хто, хто бере участь у боротьбі з ворожою кібератакою або збирає інформацію для зруйнованої війною України, повинен бути готовим захищатися від звинувачень, висунутих проти них правоохоронними органами.

Окрему увагу слід приділити ботофермам. На сьогодні 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 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 [10].

Україна перебуває у переліку країн, де з 2017 року виявили найбільшу кількість ботоферм у соціальних мережах, а у військовий час ця кількість значно зростає. У зв'язку з цим створено нові закони, які допомагають забезпечити кібербезпеку, що передбачає відповідну реакцію правоохоронних органів у разі виявлення кіберзагрози, щоб майбутні атаки не були такими успішними.

Яскравим прикладом розкриття ботоферми є викриття «мільйонної ботоферми», яка діяла «на підрив державної безпеки України» і робила це «на замовлення однієї з політсил» 2-го серпня 2022 року працівниками Служби безпеки, Національної поліції та Офісу генпрокурора. За даними правоохоронців, ліквідована ботоферма налічувала майже мільйон технічних акаунтів, з яких, зокрема, поширювала: дезінформацію про діяльність вищого військово-політичного керівництва країни; фейкові новини щодо ситуації з фронтів; інформаційні диверсії про нібито конфлікт між керівництвом ОП і головнокомандувачем ЗСУ; кампанію з дискредитації першої леді [11].

Висновки. Підсумовуючи увесь викладений матеріал стосовно кіберзлочинності під час війни та ролі ботоферм, слід сказати, що усі кібердіяння в даний час, намагаються налаштувати населення проти державної влади. Таким чином, метою діяльності проросійських ботоферм залишається дискредитація міжнародного іміджу України та усієї системи політичної української влади. На постійній основі фіксується неабиякий бурхливий сплеск активності проросійських ботоферм у соціальних мережах.

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 розробка змін до законодавства про удосконалення кримінальної відповідальності за поширення фейкової інформації та дезінформації.

ЛІТЕРАТУРА

1. Юшков А.Г. Загрозливі тенденції використання ботоферм на шкоду державним інтересам України: Механізми запобігання та протидії. *Інформація і Право.* 2021. № 3(38) С. 90-98.
2. Кількість кібератак на Україну продовжує зростати. Держспецзв'язку. *Економічна правда*: веб-сайт. URL: https://www.epravda.com.ua/news/2022/11/10/693694/ (дата звернення: 03.11.2022).
3. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text (дата звернення: 02.11.2022).
4. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.03.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 04.11.2022).
5. Microsoft відбила кібератаки на Україну. Йдеться про російську хакерську групу Strontium. *DOU KOLO.* URL: https://dou.ua/lenta/news/microsoft-repulsed-cyber-attacks-on-ukraine/ (дата звернення: 05.11.2022).
6. Хакери хотіли встановити контроль над Укртелеком: подробиці масштабної кібератаки. *Фокус*. URL: https://focus.ua/uk/digital/511551-hakery-hoteli-ustanovit-kontrol-nad-ukrtelekom-podrobnosti-masshtabnoy-kiberataki (дата звернення: 05.11.2022).
7. Кримінальний кодекс України : Закон від 05.04.2001 № 2341-III. *Відомості Верховної Ради України* (ВВР), 2001, № 25-26, ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n2493 (дата звернення: 06.11.2022).
8. Цивільний кодекс України : Кодекс від 16.01.2003 № 435-IV. *Відомості Верховної Ради України* (ВВР), 2003, №№ 40-44, ст.356. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 06.11.2022).
9. Курбан О. Фейки у сучасних медіа: ідентифікація та нейтралізація. *Бібліотекознавство. Документознавство. Інформологія*. 2018. № 3. С. 96-103.
10. 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 (дата звернення: 10.11.2022).
11. 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:10.11.2022).