DOI https://doi.org/10.36059/978-966-397-377-7-154

ЗМІНИ ЗАКОНОДАВСТВА УКРАЇНИ ЩОДО БЕЗПЕКИ У КІБЕРПРОСТОРІ В УМОВАХ ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ

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

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 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.

[1] Кількість кібератак наУкраїну 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

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

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.

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 законопроект № 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».

Закон «щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24 березня 2022 р. № 2149-IX набрав чинності 3 квітня 2022 р.

Згідно з ч. 6 ст. 361 Кримінального кодексу України (далі – КК), «Дії, передбачені частинами першою – четвертою цієї статті, не вважаються несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж»[4].

Прикінцеві положення Закону вимагають від Кабінету Міністрів розробити та забезпечити введення в дію у місячний строк з дня прийняття цього Закону (тобто до 24 квітня 2022 р.) порядку пошуку та виявлення потенційних вразливостей інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Проте лише майже через рік 16 травня 2023 року Постановою Кабінету Міністрів України № 497 було затверджено Порядок пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, який визначає механізм здійснення пошуку та

[4] КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ. Відомості Верховної Ради України (ВВР), 2001, № 25-26, URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (далі – пошук потенційної вразливості системи).

Проте дія цього Порядку є досить обмеженою. Порядок не поширюється на інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі, в яких обробляється службова інформація та/або інформація, що становить державну таємницю, розвідувальну таємницю, банківську таємницю.

Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність (ККУ) та/або яке визнано злочином міжнародними договорами України (п. 8 ч. 1 ст. 1 Закону України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 N 2163-VIII)[5].

Тут відповідно буде конкуренція загальної та спеціальної норми закону щодо визначення по суті поняття кіберзлочину.

Станом на сьогодні, в кримінальному законодавстві України немає спеціалізованої статті, яка б передбачала кримінальну відповідальність за неправомірний або несанкціонований вплив на об’єкти критичної інформаційної інфраструктури, навмисне вживлення в програмне забезпечення закладок або люків (бекдорів), за відсутність тестування програмного забезпечення, що створює певні перешкоди під час досудового розслідування та, в майбутньому, формулюванні обвинувального акту та направлення його до суду. Зокрема, без відповідної нормативно-правової бази виникають проблеми з кваліфікацією відповідних злочинів та доведенню їх вчинення.

Варто визнати й певну неповноту закону в цій частині. Від початку війни в Україні активізувався неофіційний громадський рух кіберопору ворогові, так звана "КіберАрмія". Звичайні люди, поряд із професіоналами сфери ІТ, атакують ворога у кіберпросторі, завдаючи йому збитків та зриваючи плани. Формально такі дії можуть підпадати під ознаки складів злочинів, що передбачені ст. ст. 361, 361-1 ККУ. Ймовірно, що навіть при ініціюванні відповідного кримінального провадження проти таких осіб, правоохоронні органи та суди використовуватимуть загальні механізми їх звільнення від відповідальності, адже дії таких осіб відповідають інтересам України та українського народу та не є суспільно небезпечними. Незважаючи на це, формалізація подібного звільнення від відповідальності на рівні приміток чи окремих частин відповідних спеціальних статей ККУ є бажаною у майбутньому, аби правоохоронні органи не витрачали власних зусиль на "дружній вогонь" чи пошук юридичних шляхів його уникнення.

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

Проте слід врахувати, коли відбувається несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж об'єктів критичної інфраструктури в обстановці військових подій, і це призводить до серйозних збоїв у забезпечення життєдіяльності суспільства та відсічі ворога в такий час, то, без сумніву, під час кваліфікації вчиненого ця обтяжуюча обставина має враховуватися. Водночас, цікаво відмітити, що обстановка воєнного стану чомусь не передбачена в інших комп'ютерних злочинах. При такому підході кримінально-правовий захист інформаційного простору має якийсь фрагментарний характер.

Верховною Радою України 16 січня 2024 року прийнятий в першому читанні за основу проект Закон України «Про внесення змін до Кримінального кодексу України щодо встановлення кримінальної відповідальності за несанкціоноване втручання, збут або розповсюдження інформації, що оброблюється в публічних електронних реєстрах та посилення кримінальної відповідальності під час дії воєнного стану за кримінальні правопорушення у сфері використання інформаційно-комунікаційних систем» (реєстр. № 10242).

Метою законопроекту є встановлення кримінальної відповідальності за несанкціоноване втручання, збут або розповсюдження інформації, що оброблюється в публічних електронних реєстрах, та посилення кримінальної відповідальності під час дії воєнного стану за кримінальні правопорушення у сфері використання інформаційно-комунікаційних систем. Так, змінами до Кримінального кодексу України пропонується:

– у статті 361 КК України частину першу доповнити окремим положенням щодо втручання в роботу публічних електронних реєстрів, частину п'яту доповнити кваліфікуючою ознакою «вчинення злочину службовою особою з використанням службового становища», примітку до статті доповнити новим пунктом, в якому зазначити, що під публічними електронними реєстрами у статтях 361, 3612, 362, 363, 3631 та 3652 кК України розуміються базові та інші реєстри, визначені у статті 6 Закону України «Про публічні електронні реєстри».

Висновок: підсумовуючи вище зазначене, вважаю, що Україні необхідно структурувати понятійний апарат у сфері несанкціонованого втручання в роботу телекомунікаційних та комп'ютерних мереж, ввести відповідальність за кібертероризм.