УДК 343.412

КАРЄВ І.Ю., *магістр права.*
ФУРАШЕВ В.М., *кандидат технічних наук, старший науковий співробітник, доцент,* КПІ ім. Ігоря Сікорського.

КІБЕРСТАЛКІНГ: ВІДОБРАЖЕННЯ У НАЦІОНАЛЬНОМУ ЗАКОНОДАВСТВІ

Анотація. *Стаття присвячена кіберсталкінгу – виду специфічного кіберзлочину, при якому психологічний тиск на жертву відбувається за допомогою ІТ-технологій, та його відображення у національному законодавстві.*
Ключові слова: *інформаційне суспільство, соціальні мережі, кіберсталкінг, закон.*

Summary. *The article is devoted to cyberstalking – a type of specific cybercrime in which psychological pressure on the victim occurs with the help of IT-technologies, and its reflection in national legislation.*
Keywords: *information society, social network, cyberstalking, law.*

Аннотация. *Статья посвящена кіберсталкингу – виду специфического киберпреступления, при котором психологическое давление на жертву происходит с помощью ІТ-технологий, и его отображение в национальном законодательстве.*
Ключевые слова: *информационное общество, социальные сети, кіберсталкинг, закон.*

Постановка проблеми. Кіберсталкінгом, або онлайн-сталкінгом називають переслідування в соцмережах Інтернету [1]. Кіберсталкінг – це відносно нове явище, яке виникло з розвитком інформаційних технологій. Сам термін уперше з'явився на початку 2000-х років, а в 2015 році був офіційно внесений у нову редакцію словника Уебстера, який уважається самим повним сучасним американським словником англійської мови. По суті кіберсталкінг являє собою нав'язливе переслідування в Інтернеті з боку однієї людини або групи осіб, яке несе в собі потенційну погрозу психологічному, фізичному або матеріальному стану жертви. Воно може містити в собі прямі або непрямі погрози, шантаж, несанкціоноване використання персональних даних, поширення наклепу та ін. Кіберсталкери географічно не обмежені деяким районом, країною – вони можуть переслідувати жертв, навіть перебуваючи в інших країнах з такою ж легкістю, якби вони знаходились по сусідству. Більше того, новітні технології дозволяють віртуальному переслідувачеві не тільки загрожувати іншій особі, але й підбурювати до таких дій третю сторону. І це вкрай складно відстежити. Кіберсталкінг може проявлятися не тільки в несанкціонованому використанні персональних даних з метою заплямувати честь жертви або вкрасти майно, але й в психологічному тиску, що припускає контакт із переслідувачем.

Згідно даним Міністерства юстиції США, щорічно жертвами Інтернет-переслідування стають більш 1 мільйона жінок і 370 тисяч чоловіків. Кожна 12-та жінка й кожний 45-й чоловік зіштовхуються із проявами кіберсталкінгу, спрямованого проти них. Онлайн-сталкери можуть, зокрема, зламувати акаунти, читати листування жертви, погрожувати в приватних повідомленнях, розсилати іншим знайдені в переписці інтимні світлини ("чутливі дані") тощо. Ці цифри й фактори виглядають досить тривожно. Особливо враховуючи той факт, що поки не існує достатнього досвіду боротьби з кіберсталкінгом, що утрудняє притягнення злочинців до відповідальності. Важливим є те, що віртуальне переслідування нерідко плавно перетікає в реальне. І наслідки цього можуть бути абсолютно непередбачуваними [2].

До вказаного слід зазначити, що кіберсталкінг, як сучасний поширений у світі вид злочину у сфері ІТ-технологій, поки що, на превеликий жаль, не має відображення у законодавстві України.

Метою статті є дослідження кіберсталкінгу як об'єкту інформаційної загрози.

Виклад основного матеріалу. Кіберсталкінг – вид правопорушення в інформаційній сфері, який передбачає переслідування людини в мережі з агресивним або сексуальним підтекстом, поширення неправдивих обвинувачень в Інтернеті, плітки й наклеп [3]. Він став можливим завдяки появі та розвитку декількох факторів, а саме: цифрових технологій, комп'ютерних мереж, соціальних мереж та окремої науки – соціальної інженерії [4]. Кіберсталкінг, як і його "брат" з реального світу – сталкінг (від англ. *stalk* – "переслідувати") не розглядається правоохоронцями як певний вид правопорушення (злочину), але у даному діянні існує як потерпіла сторона, так і сторона, яка певним чином створює для потерпілої сторони умови, при яких вона відчуває страх та ін. Кіберсталкерами можуть бути будь-хто, навіть просто угруповання тих, хто робить це для розваги, але легше за все виконати певні дії, коли вже маєш необхідні початкові дані.

Як зазначається у [2], США стали першої у світі країною, що розробила закон про сталкінг. Це відбулося ще 30 років тому, в 1990 році. Там кіберпереслідування підпадає під статтю закону про наклеп і утиск. Залежно від ваги злочину, розміру економічного збитку, заподіяного діянням, кримінального минулого підсудного й багатьох інших факторів порушникові може бути призначений штраф і тюремне ув'язнення. Навіть нетривалий доведений кіберсталкінг, який задав фізичної, фінансової, репутаційної або емоційної шкоди жертві, карається кримінальним судом США. Але труднощі полягають у тому, що довести такі злочини буває складно. Головні труднощі виникають в пошуку злочинця, оскільки кіберсталкери найчастіше використовують спеціальні програми, які маскують справжню IP-адресу комп'ютерного обладнання.

Механізм кіберсталкерської атаки можливий у кількох сценаріях:

1. Взаємодія безпосередньо з жертвою – варіант шантажу. Такий вид кіберсталкерської атаки проводять у тому випадку, коли жертву починають шантажувати та примушувати до здійснення певних дій, або з метою отримання певних благ як матеріального, так і не матеріального характеру для себе або третьої особи. Результату добиваються завдяки погрозам оприлюднити певну приватну інформацію про жертву, завдяки якій остання опиниться у вразливому становищі. Інструментами такої взаємодії є: листи з погрозами на електронну пошту від анонімних джерел, листи з погрозами від новостворених акаунтів у соціальних мережах, телефонні дзвінки та СМС-повідомлення. Такий варіант можливий за умови, що атакуюча сторона не впевнена у стійкості жертви, або відсутністю певної інформації, яку можливо оприлюднити. Зазвичай даний метод використовують починаючі кіберсталкери бо вони можуть бути досить швидко ідентифіковані за електронними адресами, номерами телефонів.

2. Взаємодія безпосередньо з жертвою – варіант з метою отримання контролю над соціальним життям жертви у комп'ютерній мережі. Це – видозмінений варіант шантажу. Даний вид правопорушення здійснюється за умов наявності певних технологічних навичок у нападника, зокрема, злам профілю у соціальних мережах, анонімні дзвінки, отримання контролю над усіма можливими пристроями жертви та виконання певних програм по залякуванню. Для прикладу роздрукування на принтері будь-яких словосполучень або "гра" зі світлом за умови отримання доступу до системи "розумний дім". Використання такого варіанту можливе з метою отримання коштів від жертви у обмін на залишення у спокої або для спонукання до певних дій.

3. Жорсткий пресинг жертви. Сам варіант такої взаємодії можливий за умови, що кіберсталкер має певну команду професіоналів у цій сфері або замовив виконання визначених дій "зовнішнім" професіоналам. У такому випадку інформація, яка може бути оприлюднена, у разі не досягнення визначеної мети, дійсно існує. Вона була отримана від самої жертви або іншим шляхом – з реєстрів, банків даних, або навіть інформація з обмеженим доступом. Існує вірогідність, що жертва має цінну інформацію або має зробити дещо, що має серйозне значення для замовника. Кожен крок людини у цифровій мережі відслідковується. Зловмисники отримають доступ та викрадають не тільки профілі соціальних мереж, та паролі до електронних скриньок, а ще починається фаза стеження та взаємодія у реальності. У жертви зникають гроші з розрахункових рахунків, до неї доставляють певного роду предмети, досить часто крадуть авто. Іноді для повного розпечення самої жертви зламують телефон та блокують його вихідні дзвінки або навіть створюють DDOS-атаку за допомогою СМС-повідомлень, або анонімних телефонних дзвінків.

4. Використання контактної інформації соціальної мережі. Варіант, коли у соціальних мережах певні акаунти розповсюджують завідомо неправдиву інформацію, покликану викликати огиду до жертви. У даному варіанті кіберсталкер створює велику кількість профілів у соціальній мережі, певні веб-сайти з фіктивною інформацією про жертву (при чому оплату за хостинг та ім'я сайту вносить анонімним методом або за допомогою кардінгу). Жертві пишуть у соціальні мережі та на електронну пошту свої вимоги для зупинення акції залякування. При такому варіанті ніколи не відбувається контактів у реальному світі кіберсталкера та жертви.

5. Взаємодія з знайомими з реального життя. Досить цинічний вид кіберсталкера, коли жертва не отримує погроз у прямий спосіб. Уся взаємодія проходить з жертвою через рідних та знайомих, яких починають тероризувати телефонними спам-дзвінками з анонімних номерів та наговорювати на жертву. У соціальних мережах на сторінці кожного знайомого чи рідного будуть з'являтися спам-повідомлення від новостворених акаунтів. Іноді, як варіант, замість дзвінків використовують СМС-спам. Взаємодія напряму з жертвою не відбувається. Усі вимоги зловмисники надають у СМС-повідомленнях або на сторінках у соціальних мережах усіх знайомих та рідних.

6. Масовий пресинг. Варіант жорсткого пресингу жертви, але існує досить серйозна відмінність – абсолютно усі знайомі з соціальних мереж та реального життя будуть знаходитися під атакою кіберсталкера. Можливий варіант, що і найближчі родичі втратять кошти з розрахункових рахунків.

Для виконання будь-якого з варіантів необхідно пройти кілька стадій підготовки правопорушення, але за умови, що коли вони будуть проходити у кіберпросторі, то будуть мати свої особливості та специфіку:

1). Вибір жертви. За умови, що жертва вже знайома, тоді дана стадія переходить у наступну. Якщо жертва не знайома – обирається з соціальних мереж за певним критерієм, який визначений вже кіберсталкером.

2). Стадія розвідки. Вся інформація, яку можливо отримати з соціальних мереж – збирається та класифікується. Спочатку збирається інформація про електронну адресу, контактну інформацію, місце життя, контакти у соціальних мережах, з'ясовується ступінь взаємовідносин, роль у взаємовідносинах. Найбільший пріоритет надається рідним та тим, з ким людина взаємодіє постійно, де працює та детальна інформація про хобі. Якщо людина не відома, то збирається інформація про її матеріальний стан.

3). Стадія слідкування. Можливий варіант коли винаймається приватний детектив, що починає слідкувати за потерпілою особою. Але основне слідкування йде у соціальних

мережах. До сфери інтересів входить – персональні дані, приватне життя, часто відвідувані місця, рухоме майно, інформація про номери рахунків та банки, клієнтом яких є жертва та ін.

4). Тиха взаємодія або глибинне слідкування. Відбувається злам профілю соціальної мережі та електронного поштового ящику. Отримується доступ до карткових та розрахункових рахунків жертви, якщо така дія є у плані кіберсталкера.

5). Активна фаза. Початок обраного сценарію нападу на жертву. Отримання перших погроз.

Існує й інший вид кіберзлочину – кібербуллінг співзвучний з кіберсталкінгом. Є думка, що кіберсталкінг та кібербуллінг – одне й те саме, але це зовсім різні методи впливу та взаємодії з жертвою. Об'єднує ці два вида правопорушень використання одних і тих же засобів – апаратно-програмних засобів, таких як месенджер, соціальна мережа, також існує жертва та нападник. Але природа та кінцева мета досить різні. Якщо кіберсталкінг – це систематичний, моральний та психологічний тиск на жертву для отримання певного результату, то кібербуллінг – цькування для задоволення певних морально-психологічних потреб нападника [5 – 7].

На жаль, до цього часу національним законодавством не розглядається сталкінг та кіберсталкінг як окремий вид правопорушень. Не створені механізми фіксації, підтвердження та збору доказів, а також захисту жертви. Але при цьому слід враховувати, що кіберсталкінг – це кіберзлочин, тобто складне правопорушення, що складається з кількох дій, які мають певний сценарій та використовують апаратно-програмні засоби. Також слід враховувати, що певні закони поки ще не адаптовані під сучасні реалії, тому у них не означена юридична відповідальність за здійснення подібних діянь. Тому досить важко визначити ступінь вини організатора діяння, але такий злочин необхідно розглядати по частинах, адже він виконується у залежності від сценарію.

Основна ідея кіберсталкінгу – втручання у життя певної фізичної особи за допомогою комп'ютерної мережі для створення умов морального, матеріального впливу та психологічного страждання жертви. Кримінальним законодавством України зазначені дії не визначаються [8]. Крім цього, у випадку, коли людині не погрожують видати певні про неї матеріали або не наказують перевести кошти для зупинення акції, немає вимог виконати певні дії – лише цькування та постійне життя у страху, то такий випадок законодавцем, на жаль, також не визначено. Також не визначено протиправними діяння осіб, які за допомогою комп'ютерної мережі та смартфонів здійснюють надокучливі дзвінки або СМС-повідомлення з погрозами, шантажем, вимаганнями тощо, які повинні розглядатися як явний злочин в інформаційній сфері.

Немає чіткого розуміння, що таке DDOS-атака на пристрій зв'язку потенційної або реальної жертви за допомогою великої кількості телефонних дзвінків. По своїй суті таке порушення, як залякування особи завдяки засобам зв'язку, не визначено жодним законом.

В умовах розвитку цифровізації поняття "персональні дані" та його сприйняття що існує у чинному у законодавстві України, стає дедалі більш "розмитим" та неоднозначним. Більш того, відсутня чітка межа між поняттями "персональні дані" та "конфіденційна інформація" (яке у законодавстві взагалі не визначено), а також немає чіткої юридичної відповідальності за недбалість поводження з персональними даними на всіх етапах роботи з ними – збору, обробки, поширення, збереження та знищення [9].

Якого плану інформацію про особу треба вважати конфіденційною інформацією?

Якщо інформація взята з соціальних мереж, тобто та, яку особа власноруч виклала, то така інформація вже є публічною та загальнодоступною.

Якщо особу шантажують розповсюдженням інформації еротичного характеру або розповсюдженням інформації та доказів стосовно її приватного життя, яку б вона хотіла б приховати, то отримаємо ситуацію, коли відсутність реагування на це з боку правоохоронних органів "відштовхують" людину і провокують злочинців на кіберсталкерську активність. Як приклад інформації, з якою людина за власним бажанням не звернеться до правоохоронних органів – докази її участі в кримінальному правопорушенні, які не були отримані правоохоронцями, матеріали еротичного характеру, певний компромат та інші.

Фізичну особу, яка являє собою потерпілу сторону, такий підхід як законодавця, так і правоохоронців ставить у заздалегідь програшне положення, адже відсутній механізм правового захисту від злочинних дій подібного роду. Досить часто інформацію використовують як товар (що також у законодавстві не визначено), як засіб для маніпуляції, і у жодному випадку немає варіанту заборонити та вилучити інформацію у злочинця.

Для отримання контролю над соціальними мережами, електронною адресою та комп'ютерним обладнанням зловмисники проводять певні заходи, а саме процес зламу. Навіть за умови, що людина певним чином запідозрить спроби зламу – потерпілому нікуди звернутися з даною проблемою, адже жодна відповідна правоохоронна структура не працює з злочинами на етапі спроби зламу. Навіть після зламу електронної пошти, зламу та отримання контролю за розрахунковим рахунком жертва не може зробити майже нічого. Служба безпеки банку – буде відписуватися, що клієнт повинен самостійно дбати про власну безпеку, при зверненні до кіберполіцію – там теж активних дій не проглядається. Доказування через суд – справа не одного місяця, навіть якщо вдасться довести свою позицію, то завдяки інфляції людина отримає вже збитки та витрачений час.

Проблема кіберсталкінгу загострюється і надалі буде загострюватися в умовах подальшого активного розвитку комп'ютерних мереж та активного інтегрування комп'ютерних технологій у суспільне та приватне життя. Якщо вчасно не провести модернізацію законодавства у сфері захисту інформації та персональних даних, не створити державну службу, обов'язком якої буде робота щодо правопорушень, у ході яких за допомогою програмно-апаратного комплексу виконуються операції з отримання доступу та контролю над програмним забезпеченням постраждалої сторони, то з подальшою інтеграцією комп'ютерних технологій у приватне та соціальне життя отримаємо зростання кількості кіберзлочинців, які зможуть вільно тероризувати населення, відчуваючи свою безкарність.

Висновки.

Сучасні юридичні проблеми у сфері електронно-інформаційної комунікації пов'язані з тим, що техніко-технологічна взаємодія з реальним світом здійснюється через віртуальний простір за допомогою певного програмно-апаратного комплексу.

У зв'язку зі швидким розвитком ІТ-технологій та повільним розвитком законодавства щодо сфери комп'ютерних технологій маємо реальну ситуацію, коли злочинці діють безкарно, за умов недосконалості законодавства.

Складність вияву злочинця та отримання допомоги від кіберполіції, відсутність законодавчого визначення понять "кіберсталкінг" та "кібербуллінг" разом з визначенням механізмів протидії, надає злочинцям можливість безкарно виконувати дії, які вони обирають за певним сценарієм. Саме велика кількість варіацій дій злочинця не дає можливості чітко визначити ступінь його вини, а потерпілій стороні – навіть можливості на мінімальний захист від зловмисника. Зокрема це стосується відсутності сталих механізмів взаємодії та нормативних важелів щодо банківських структур, які

зобов'язують забезпечувати більше тісну взаємодію з правоохоронними структурами у частині розслідування втрати коштів з розрахункового рахунку потерпілих.

У підсумку, масштаб та поява нових способів і методів кіберзлочинів зумовлює потреби подальших досліджень з цієї тематики, спрямованих на удосконалення та розвиток національного законодавства, створення спеціальних програмних засобів захисту прав людини та відповідного методичного забезпечення для сфери протидії кіберзлочинності.

Використана література

1. Про сталкінг… URL: https://bit.ua/2020/01/pro-stalking

2. Меня преследуют в Интернете: что такое кибersталкинг, и как от него защититься. URL: https://www.marieclaire.ru/stil-zjizny/menya-presleduyut-v-internete-chto-takoe-kiberstalking-i-kak-ot-nego-zaschititsya

3. Кібersталкінг. URL: https://stop-ugroza.ru/life/kiberstalking-i-kak-ot-nego-zashhititsya

4. Соціальна інженерія: виклики та перспективи боротьби в українському контексті. *Інтернет ресурс – Українське право*.URL: https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_demchuk_Social_engineering_perspectives_of_the_struggle_in_ukrain (дата звернення: 25.01.2021).

5. Workplace Violence. United state department of labor. URL: https://www.osha.gov/workplace-violence (дата звернення: 25.01.2021).

6. The Involvement of Girls and Boys with Bullying: An Analysis of Gender Differences. US national library of medicine. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3881143 (дата звернення: 25.01.2021).

7. Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress, Research Press, 2007. – ISBN 0878225374.

8. Кримінальний Кодекс України: Закон України від 05.04.01 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14/conv#n744 (дата звернення: 30.01.2021).

9. Закон України "Про захист персональних даних" від 01.06.10 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 30.01.2021).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~