УДК 340.155.4:343.412

БЕЖЕВЕЦЬ А.М., аспірантка Національного технічного університету України
“Київський політехнічний інститут імені Ігоря Сікорського”.
ORCID: https://orcid.org/0000-0001-5434-3883.
ШАХ К.І., студентка факультету соціології і права
“Київський політехнічний інститут імені Ігоря Сікорського”.

КІБЕРБУЛІНГ ТА КІБЕРСТАЛКІНГ В ІНТЕРНЕТ-СЕРЕДОВИЩІ: ПОРІВНЯЛЬНО-ПРАВОВИЙ АНАЛІЗ ПОНЯТЬ

Анотація. *У статті розглянуто різновиди таких правопорушень, як кібербулінг та кіберсталкінг, висвітлено проблеми, пов’язані із захистом жертв, їх психологічним станом після даних злочинів. Наведено досвід боротьби інших країн з цими явищами та запропоновано метод боротьби з кіберсталкінгом в Україні.*

Ключові слова: *кібербулінг, кіберсталкінг, онлайн-сталкінг, Інтернет, домагання, переслідування, флеймінг, настирливе переслідування, онлайн-образа, онлайн-домагання, онлайн-насильство.*

Summary. *This article explores different types of crimes such as cyberbullying and cyberstalking, highlighting the problems associated with protecting victims and their psychological state after these crimes. We studied the experience of other countries in combating these phenomena and proposed a method of combating cyberstalking in Ukraine.*

Keywords: *cyberbullying, cyberstalking, online stalking, internet, harassment, stalking, flaming, harassing pursuit, online insults, online harassment, online abuse.*

Постановка проблеми. З розвитком Інтернет-середовища відкриваються нові його можливості, як позитивні, так і негативні. Нажаль, не всі користуються соцмережами для спілкування, обміну інформацією, ідеями, думками тощо. Іноді їх користувачі використовують їх можливості для вчинення образливих дій, які мають на меті переслідування жертви, завдання їй моральних страждань та інших негативних наслідків. Такі дії отримали назву кібербулінг та кіберсталкінг.

Ці явища почали з’являтися на початку 2000-х років, тоді ж вперше з’явилися і терміни. На сьогодні кібербулінг та кіберсталкінг стають все поширенішими. В наші дні, коли Інтернет став незамінним і без нього неможливо уявити своє життя, окрім корисної інформації та можливості знайти матеріали для саморозвитку, популярними стали соціальні мережі та мережеві ігри. З їх появою у кожної людини з’явилась можливість знайомитись та спілкуватись в Інтернеті. Проте, іноді можна знайти друзів через мережу, а інколи можна натрапити на кібербулерів або кіберсталкерів, які шукають своїх жертв через популярні серед молоді соціальні мережі/ігрові платформи/форуми, а іноді тими самими кривдниками можуть виявитись і знайомі люди. Кібербулери та кіберсталкери ставлять жертву в жахливе некомфортне становище приниженням честі та гідності особи, порушенням особистого простору, а в деяких випадках погрозами життю та здоров’ю особи. Через даний вид Інтернет-атак дуже сильно страждає психіка жертви, іноді це призводить і до більш негативних наслідків, таких як депресія або навіть самогубство.

Метою статті є визначення поняття кібербулінгу та кіберсталкінгу, виявлення їх відмінності, небезпечного впливу, а також – методів боротьби з цими явищами на підставі порівняльного аналізу законодавства інших країн.

Результати аналізу наукових публікацій. Сьогодні багато дослідників приділяють увагу поняттям, які стосуються правопорушень в мережі Інтернет. Різні аспекти міжнародно-правових стандартів надання правової допомоги у цій сфері розглядали П. Боцій, П. Тьяден і Н. Тоенн, Д. Фута. Серед українських дослідників можна виділити роботи А.О. Ведернікової, І.Ю. Карєва та В.М. Фурашева, В.В. Маньгори та К.А. Вітковської.

Кібербулінг безсумнівно став важливою проблемою серед молоді та підлітків в останнє десятиріччя. Явище це стало більш частим у міру розширення використання підлітками електронних пристроїв зв'язку, таких як комп'ютери та мобільні телефони. Однак в даний час проводиться велика кількість заходів з попередження даного негативного явища.

Кіберсталкінг, загрози та пов'язана з цим технологія насильницької злочинної поведінки все частіше проявляється в суспільстві. Центр контролю та профілактики захворювань США повідомляє, що кожна шоста жінка та кожен 19 чоловік у Сполучених Штатах у певний момент свого життя зазнали переслідування, яке викликало у них страх або віру, що їм або близькій їм людині буде завдано шкоди чи вбито [1].

В Україні це явище почало вивчатися досить нещодавно, і для більшості населення можуть бути не зрозумілі такі поняття як кібербулінг та кіберсталкінг, тому важливим є пояснення та порівняння цих двох явищ.

При цьому, слід підкреслити, що хоча це явище є новим, слід розуміти той факт, що інші більш розвинуті країни, знайшли шлях боротьби із цими фактами протиправної поведінки, тому аналіз їх досвіду є дуже доцільним.

Виклад основного матеріалу. Для розуміння викладеного матеріалу слід розпочати з наведення визначення таких понять як "кібербулінг" та "кіберсталкінг".

Кібербулінг – це цькування повідомленнями, що містять образи, агресію, залякування, хуліганство; соціальне бойкотування за допомогою різних Інтернет-сервісів, тобто використання технологій з наміром зашкодити, розладнати або принизити будь-кого [1].

Кібербулінг може прийняти будь-яку форму від неприємних текстових та MMS-повідомлень до грубих записів у блозі або соціальних мережах, а так само електронних повідомлень і злісних сайтів, створених з метою приниження людини. Швидкість поширення неприємних повідомлень або зображення на порядок вища ніж при булінгу.

Анонімність кібербулінгу і знеособлена природа Інтернету може залучити молоду людину в діяльність, про яку вона не може подумати в реальному житті, тобто стати порушником або спостерігачем.

Різновидом кібербулінгу є флеймінг, тобто сварки-листування у вигляді обміну злими, жорстокими і грубими повідомленнями між двома і більше користувачами в публічних і приватних місцях спілкування в мережі Інтернет.

Відповідно до розробленого Національним центром жертв злочинів США в 2002 році пояснення терміну "кіберсталкінг" (*cyberstalking*) – це переслідування, яке є особливим типом злочину, що відрізняється від інших тим, що в разі переслідування віктимізації піддається одна і та ж жертва, злочин являє собою ланцюжок інцидентів різного ступеня тяжкості, які стабілізують постійний і тривалий вплив злочинця на постраждалу сторону [1].

Національний інститут юстиції США визначає переслідування як поведінку, спрямовану на конкретну людину, включаючи повторну візуальну або фізичну близькість, небажане спілкування (без згоди) або усну, письмову або непряму загрозу, або їх комбінацію, що може викликати обґрунтований страх [2].

Переслідування направлено на безпеку потерпілого, переслідування робить людину жертвою, викликаючи страх, невпевненість, неспокій, почуття безпорадності, нестабільності, тривоги, емоційний дискомфорт, стрес і повну дестабілізацію повсякденного життя. Переслідування може бути пов'язано з усіма формами насильства аж до вбивства. Переслідувачами можуть бути як колишні, так і нинішні члени сім'ї, знайомі або зовсім незнайомі люди, які думали, що їх з жертвою пов'язують тісні відносини. Справи про переслідування в світі визнаються дуже складними як з точки зору розкриття і розслідування злочинів, так і з точки зору фактичного припинення злочинної діяльності, оскільки переслідувачі, як правило, настільки захоплені своєю ідеєю, що вони не бояться отримати покарання і потім продовжують свою злочинну діяльність. Адвокати обвинувачених в переслідуванні часто пояснюють поведінку своїх підзахисних обсесивно-компульсивними розладами, для яких характерна ірраціональна поведінка і параноїдальні тенденції. Проти цього заперечують організації, що захищають жертв, засновуючи свою думку на тому факті, що в основному всі злочинці в судово-психіатричній експертизі визнаються осудними і здатними усвідомлювати і керувати своїми діями.

З метою переслідування обраної жертви можуть застосовуватися злочинні дії проти персональних даних фізичних осіб, зокрема, викрадення засобів ідентифікації особистості. Викрадені або підроблені засоби ідентифікації особистості можуть слугувати інструментом для переслідування. У світовій практиці є багато прикладів, коли доступ до персональних даних здійснюється спеціально для переслідування жертви, використовуючи отриману інформацію для здійснення небажаних телефонних дзвінків, порушення спокою тощо. Зв'язок між незаконною діяльністю з персональними даними фізичних осіб і переслідуванням дуже тісний, оскільки фактично не отримавши необхідні дані, переслідувач не зможе виконувати всі інші заплановані дії щодо цькування обраної жертви.

Одним з видів переслідування, які створюють серйозну загрозу даним фізичних осіб, є віртуальне кібер-переслідування (кіберсталкінг), для якого, як і для переслідування в реальному житті, характерно домагання (harassment) і одержимість переслідувача своєю жертвою. Кіберсталкінгом, або онлайн-сталкінгом називають переслідування в соцмережах Інтернету [3]. Переслідування може фактично розглядатися як форма цього незаконного домагання.

Зміст цього правопорушення включає в себе відстеження незнайомої або знайомої людини у віртуальному середовищі, соціальних мережах, небажане спілкування з людиною, домагання, відправку недоречних пропозицій у вигляді SMS, електронною поштою, в соціальних мережах, залякування (за допомогою телефонних дзвінків або різних електронних листів тощо), а також цілеспрямована дискредитація людини у віртуальному середовищі (відправлення повідомлень від її імені іншим особам, створення фальшивих профілів тощо), очорнення шляхом поширення неправдивої інформації про людину (наприклад, розміщення оголошень про надання інтимних послуг із зазначенням персональних даних, адреси, номера телефону потерпілого). Кібер-переслідування може виражатися у прихованій фотозйомці людини, спостереженні або прослуховуванні (включаючи віддалений доступ до комп'ютера потерпілого, розміщення прихованих камер в будинку жертви тощо).

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 [4].

Каліфорнія стала першим штатом в Сполучених Штатах Америки, в якому з 1 січня 1999 була введена кримінальна відповідальність за кібер-переслідування. Слід зазначити, що саме в Каліфорнії в тому ж році широкого резонансу набула справа Гері Деллапента (Gary Dellapenta), звинуваченого в кібер-переслідуванні, який був засуджений до шести років тюремного ув'язнення за особливу форму переслідування, так званого "переслідування через посередника" (*stalking by proxy*) [5]. В цьому випадку переслідувач використовує інших осіб для залякування. Так, Деллапент отримавши відмову від жінки, з якою він хотів встановити тісні відносини, хотів помститися, і від імені цієї жінки виклав кілька рекламних оголошень на сумнівних Інтернет-сайтах, в яких вказав, що хоче реалізувати свої еротичні фантазії, пов'язані з груповим статевим актом, зґвалтуванням тощо. В оголошеннях була точно вказана домашня адреса, телефон жінки і код безпеки вхідних дверей, який Деллапент дізнався, використовуючи свою посаду в охороні. Потерпілу стали переслідувати ті, хто відгукнувся на рекламні оголошення, як по телефону, так і з'явившись за місцем проживання. Потерпіла була змушена покинути своє житло і протягом тривалого періоду ховатися, поки Деллапент не був арештований, і переслідування припинилося [6].

У 2016 році в засобах масової інформації набула широкого розголосу кримінальна справа, в якій за кібер-переслідування і крадіжку особистих даних був засуджений 31-річний громадянин США Майкл Даніель Рубенс (Michael Daniel Rubens) [7]. Він був засуджений до тюремного ув'язнення на десять років і штрафу в розмірі $10000 США. М.Д. Рубенс звинувачений в тому, що з 2012 по 2015 рік, перебуваючи за своїм місцем проживання, використовуючи спеціальну комп'ютерну програму для приховування IP-адреси, він зламав десятки Інтернет-профілів жінок, в тому числі електронну пошту і сторінки соціальних мереж, та незаконно отримав їх фотографії і особисті дані. Отримані зображення він використовував для створення порнографічного матеріалу, який далі публікував на різних веб-сайтах в Інтернеті. Серед жертв Рубенса було багато його знайомих жінок, в тому числі колишні однокласниці, колеги, друзі друзів. Рубенс створив електронну папку для кожної своєї жертви з тисячами файлів з приватною інформацією (відомості про сім'ю, адреси, робочі місця тощо). Він ретельно збирав і зберігав ці дані про кожну з постраждалих жінок. Зібрані персональні дані і створені порнографічні матеріали Рубенс використовував, щоб протягом багатьох років шантажувати, ображати і принижувати свої жертви. Суддя, який розглядав цю справу, підкреслив, що настав час усвідомити, що кібер-переслідування в наші дні є дуже серйозним злочином.

В Латвії переслідування не визнавалося окремим кримінальним злочином до червня 2017 року, коли були внесені поправки в Кримінальний Закон (далі – КЗ Латвії), доповнивши його новою статтею 132.1 "Переслідування" в такій редакції: "За неодноразове або тривале переслідування іншої особи, стеження за нею, погрози на її адресу або спроби вступити з нею в небажаний зв'язок, якщо у неї були підстави побоюватися за своє життя або за життя своїх близьких, передбачено покарання у вигляді короткострокового позбавлення волі або примусових робіт, або грошового штрафу" [8].

Хоча кібер-переслідування входить до складу переслідування, проте в статті 132.1 КЗ Латвії вказане визначення складу переслідування із зазначенням тільки чотирьох

видів дій, які не включають всі можливі підвиди кібер-переслідування. Крім того, в анотації самого законопроєкту вказується, що "оскільки методи переслідування можуть відрізнятися і в ході часу можуть також змінюватися з розвитком цифрових технологій, більшість країн, які визнають переслідування як кримінальний злочин, не включають до свого законодавства повний перелік дій…" [8].

Для порівняння можна розглянути передбачену в Законі про покарання Естонії кримінальну відповідальність за "настирливе переслідування" (*harassing pursuit*) [9], яке пояснюється як повторні або послідовні спроби зв'язатися з іншою особою, стежити за нею або втручатися в особисте життя проти волі цієї особи в іншому вигляді, якщо метою або наслідками цього є залякування, приниження або занепокоєння особи будь-яким іншим способом (за винятком несанкціонованого контролю і стеження за іншою особою) (*unauthorised surveillance*) з метою збору інформації про цю особу, відповідальність за що передбачена в статті 137 Закону Естонії "Про покарання". Тобто в естонському законодавстві поняття "переслідування" формулюється більш широко ("або втручається в особисте життя людини проти його волі іншим способом"), передбачаючи можливість залучення до відповідальності за всі (будь-які) дії, які за своєю суттю і метою відповідають основним ознакам переслідування, в тому числі кібер-переслідування.

В анотації статті 132.1 КЗ Латвії з посиланням на 184 пункт Пояснювальної записки до Конвенції Ради Європи про попередження та боротьбу з насильством щодо жінок та домашнім насильством зазначено, що мета переслідування завжди повинна бути пов'язана з бажанням вселити страх своїй жертві. Але з цим твердженням не можна погодитися, оскільки не всі переслідувачі хочуть нашкодити і залякати жертву. Навпаки, часто переслідувач психічно не збалансований, він настільки любить свою жертву, що навіть переконаний у взаємних симпатіях. Залякування і прагнення викликати страх у таких випадках не є метою, а скоріше наслідком.

Доцільно відзначити також досвід боротьби з кібербулінгом у Японії. На даний час японське законодавство криміналізує онлайн-образи, онлайн-домагання та онлайн-насильство, тобто негативні дії, що ображають інших користувачів у соцмережах. Проте, Парламент Японії схвалив законопроєкт, який значно збільшує відповідальність за цей злочин. Якщо на сьогодні чинне законодавство передбачає для винних осіб арешт до 30 діб або стягнення штрафу до 10000 єн (еквівалент $75 США), то планується тюремне ув'язнення строком до 12 місяців або штраф до 300000 єн (еквівалент $2200 США) [10].

Висновки.

З огляду на наведене вище, кіберсталкінг та кібербулінг визнаються злочинами у багатьох країнах. Кіберсталкінг є більш соціально шкідливим явищем ніж кібербулінг.

Вважаємо, що згадані порушення слід віднести до інформаційних правопорушень (правопорушень в інформаційній сфері).

18 грудня 2018 року Верховна Рада України прийняла Закон "Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)". Законом було запроваджено адміністративну відповідальність за вчинення булінгу, в тому числі й із застосуванням електронних комунікацій.

На нашу думку, слід законодавчо урегулювати питання щодо кіберсталкінгу. Зокрема, визначити кіберсталкінг як неодноразове або тривале переслідування іншої особи за допомогою різних Інтернет-сервісів, та/або з використанням цифрових технологій, стеження за нею, погрози на її адресу або спроби вступити з нею в небажаний зв'язок, якщо у неї були підстави побоюватися за своє життя або за життя

своїх близьких, відчувати приниження гідності та честі, мати підстави для того, щоб відчувати себе приниженою. При цьому за цей вид порушення слід встановити кримінальну відповідальність.

На даний час Україна лише розпочинає свій законодавчий шлях в цій сфері, що, в свою чергу, потребує докладного науково-теоретичного вивчення цього питання з метою його практичного втілення у конкретні норми.

Використана література

1. Creating an Effective Stalking Protocol, the National Center for Victims of Crime, Publication supported by the Office of Community Oriented Policing Services, U.S. Department of Justice. 2002. URL: https://victimsofcrime.org/docs/src/creating-an-effective-stalking-protocol.pdf?Sfvrsn=2

2. Tjaden P., Thoennes N., National Institute of Justice, U.S. Department of Justice and Centers for Disease Control and Prevention. Stalking in America: Findings From the National Violence Against Women Survey. URL: https://catalog.hathitrust.org/Record/003795050

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

4. Карєв І.Ю., Фурашев В.М. Кіберсталкінг: відображення у національному законодавстві. *Інформація і право*. № 1(36)/2021. URL: http://www.ippi.org.ua/kar%D1%94v-iyu-furashev-vm-kiberstalking-vidobrazhennya-u-natsionalnomu-zakonodavstvi-s-29-34

5. Bocij P. Cyberstalking: Harassment in the Internet Age and how to Protect Your Family. London, 2004. 288 p.

6. Foote D. You could get raped. *Newsweek*. 1999. URL: http://www.newsweek.com/you-could-get-raped-168972

7. Cyberstalker Sentenced to 10 Years in Prison Department of Justice. 2016. URL: https://www.justice.gov/usao-ndfl/pr/cyberstalker-sentenced-10-years-prison

8. Поправки к Уголовному закону: законопроект (794/Lp12). URL: http://titania.saeima.lv/LIVS12/SaeimaLIVS12.nsf/0/1995DC23D08AA716C225808E002F9306?OpenDocument#a

9. Penal Code of the Republic of Estonia, § 157^3. URL: http://www.legislationline.org/ documents/section/criminal-codes

10. В Японії онлайн-образи караються. URL: https://edition.cnn.com/2022/06/14/asia/japan-cyberbullying-law-intl-hnk-scli/index.html

11. Ведернікова А.О. Кримінологічна характеристика кібербулінгу та його видів. *Інформація і право*. № 3(38)/2021. С. 99-108.

12. Маньгора В.В., Вітковська К.А. Особливості юридичної відповідальності за прояви булінгу та шляхи боротьби з ним. *Інформація і право*. № 1(40)/2022. С. 97-110.

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