2001. С. 180-185.
3. Кічігіна Є.В. Кримінальне право БРСР. Мінськ, 1981. 380 с.
4. Ковальов М.І. Співучасть у злочині. Види співучасників і форми участі в злочинній діяльності. Свердловськ, 2008. 197 с.
5. Савченко А.В., Кузнєцов В.В., Штанько О.Ф. Сучасне кримінальне право україни: курс лекцій. Київ: Атіка, 2013. 470 с.
6. Тельнов П.Ф. Відповідальність за співучасть у злочині. Москва, 1974. 120 с.
7. Хакімов І.Х. Правові питання співучасті. Ташкент, 1983. 107 с.

УДК 343.9(043.2)

Гопкало І. І., студентка,
Національний авіаційний університет, м. Київ, Україна
Науковий керівник: Грекова Л.Ю., асистент

КОМП'ЮТЕРНІ ЗЛОЧИНИ: КРИТЕРІЇ КРИМІНАЛІСТИЧНОЇ КЛАСИФІКАЦІЇ

Поняття «кіберзлочинність» вперше з'явилося в американській, а потім і в іншій іноземній літературі на початку 1960-х рр. і визначалося як порушення чужих прав та інтересів стосовно автоматизованих систем обробки даних. Кіберзлочинність (англ. cybercrime) – це поняття, яке охоплює комп'ютерну злочинність та інші зазіхання, де комп'ютер є знаряддям або способом злочину проти власності, авторських прав, громадської безпеки, моралі тощо [1, с. 338].

Найбільш поширена класифікація кіберзлочинів нині ґрунтується на Конвенції Ради Європи про кіберзлочинність, у цьому документі кіберзлочини поділяються на п'ять груп: 1) злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему, нелегальне перехоплення комп'ютерних даних); 2) злочини, пов'язані з використанням комп'ютера як засобу скоєння злочинів, а саме – для маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерні підроблення); 3) злочини, пов'язані з контентом (змістом даних); 4) злочини, пов'язані з порушенням авторського права і суміжних прав; 5) акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж [2].

В залежності від характеру вчинення кіберзлочинів В.В. Голіна та Б.М. Головкін виділяють такі їх групи: агресивні – кібертероризм, погроза фізичної розправи (наприклад, передана через електронну пошту), кіберсталкінг (переслідування іншої особи через Інтернет), дитяча порнографія (створення порнографічних матеріалів із зображенням дітей, розповсюдження цих матеріалів); неагресивні – кіберкрадіжка,

кібервандалізм, кібершахрайство, кібершпигунство, створення фіктивних WEBсайтів розповсюдження спаму та троянських програм, перехоплення трафіку тощо) [3, с. 332].

У той же час, з урахуванням мотивації злочинців О.М. Пфо умовно розділяє такі злочини на наступні категорії: кібершахрайство з метою заволодіння коштами (шахрайство в мережі Інтернет, зокрема: створення «фінансових пірамід» в мережі Інтернет, підробка платіжних карток і банкоматне шахрайство); кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу); втручання в роботу інформаційних систем з метою отримання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення шкоди конкурентам) [4, с. 33].

Одним із різновидів кіберзлочинів є піратство – несанкціоноване копіювання, поширення та продаж об'єктів авторського права, яке вчиняється способами:

– класичне комп'ютерне піратство – контрафактні або «кустарні» (самостійно виготовлені) диски, встановлення програмного забезпечення (далі ПЗ) на замовлення невідомими «спеціалістами» (які не є представниками компанії-розробника);

– злом програми за допомогою спеціального класу ПЗ (crack, keygen) – їх встановлення із метою зняття обмежень у програмному продукті, пов'язаних із вбудованим захистом від неправомірного використання.

В.О. Мещеряков пропонує ще одну підставу для класифікації кіберзлочинів за об'єктом злочинного посягання – комп'ютерною інформацією, а саме: знищення (порушення) комп'ютерної інформації; неправомірне заволодіння комп'ютерною інформацією чи порушення виключного права на її використання [5, с. 76].

У Кримінальному кодексі України Розділом 16 Особливої частини передбачена кримінальні відповідальність щодо злочинів у сфері використання електроннообчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Розглядаючи питання про кримінальну відповідальність за кіберзлочини, А.А. Музика і Д.С. Азаров зазначають, що у широкому розумінні у ч. 3 ст. 190 ККУ (шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки), та окремими суспільно небезпечними діями, передбаченими, зокрема, ст. 200 ККУ (незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення), ст. 176 (порушення авторського права) тощо, мова також йде про злочини цієї категорії [6, с. 52].

Отже, зростання інформаційних технологій зумовлює не тільки прогресивні зміни в економіці, але й негативні тенденції розвитку злочинного світу, появу нових форм і видів злочинних посягань і тому

питання безпеки кіберпростору, боротьби з кіберзлочинністю є актуальним як на міжнародному рівні, так і на рівні окремої країни, потребує подальшого розгляду і вивчення науковою спільнотою.

Література

1. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби. *Теоретичні та прикладні питання економіки*. М-во освіти і науки України, Київ. нац. ун-т ім. Тараса Шевченка, Ін-т конкурентного сусп-ва; зб. наук. пр. Київ: Вид.-поліграф. центр «Київ. ун-т», 2009. Вип. 19. С. 338–342.

2. Конвенція про кіберзлочинність. № 994_575 від 23.11.2001 р. Ратифікована від 07.09.2005. URL: https://zakon.rada.gov.ua/ laws/show/ 994_575#Text.

3. Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини. Навчальний посібник. Харків: Право, 2014. 513 с.

4. Пфо О.М. Основні поняття і класифікація кіберзлочинності. Актуальні задачі та досягнення у галузі кібербезпеки. Матеріали Всеукр. наук.-практ. конф., 23–25.11.2016 р. Кропивницький: КНТУ, 2016. С. 33-34.

5. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. … д-ра юрид. наук. Воронежский государственный университет, 2001. 386 с.

6. Музика А.А. Законодавство України про кримінальну відповідальність за «комп'ютерні» злочини: науково-практичний коментар і шляхи вдосконалення. Київ: Вид. Паливода А.В., 2005. 120 с.

УДК 343(043.2)

Гуменюк К. М., студентка,
Хмельницький університет управління і права ім. Леоніда Юзькова,
м. Хмельницький, Україна
Науковий керівник: Плисюк Н. М., к.ю.н., доцент

ОБ'ЄКТИВНА СТОРОНА ЗЛОЧИНУ, ПЕРЕДБАЧЕНОГО СТАТТЕЮ 307 ККУ

До незаконного обігу наркотичних засобів, психотропних речовин і прекурсорів належать злочини, передбачені ст.ст. 305-320 Кримінального кодексу (далі - КК) України, а також певні дії (чи бездіяльність), передбачені КУпАП [1].

Об'єктивна сторона складу злочину, передбаченого ст. 307 КК України визначає такі дії: незаконне виробництво, виготовлення, придбання, зберігання, перевезення чи пересилання з метою збуту, а також незаконний збут наркотичних засобів, психотропних речовин або їх аналогів. Для наявності складу злочину досить вчинення хоча б однієї із зазначених дій. Визнання передбачених ч. 1 ст. 307 КК України альтернативних видів злочинної поведінки одним злочином мало б