Мартинова Н.О.
студентка,
Науковий керівник: **Великанова М.М.**
кандидат юридичних наук, доцент,
доцент кафедри правознавства,
Київський національний торговельно-економічний університет

ОСОБЛИВОСТІ КВАЛІФІКАЦІЇ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРНОЇ ТЕХНІКИ

Поряд з появою та розвитком всесвітньої мережі Інтернет, а також масовим використанням засобів комп'ютерної техніки як засобів комунікації, виробництва й автоматизації більшості процесів життєдіяльності, з'явилась і нова особлива форма злочинності. У теорії та практиці проблематика злочинів із застосуванням комп’ютерних інформаційних технологій отримала умовну узагальнену назву “комп’ютерна злочинність”, або, відповідно до міжнародної термінології “кіберзлочинність”. Проте чинний Кримінальний кодекс України такого поняття не містить, і доцільність введення такого поняття до національного законодавства є дискусійною.

На сьогоднішній день, терміни «кіберзлочинність», «хакери», «комп’ютерний злом», «крадіжка машинного часу» вже перестали бути екзотикою для юристів. Адже комп’ютерні злочини – це одна з найдинамічніших груп суспільно небезпечних посягань. Дуже швидко збільшуються показники поширеності даних злочинів, а також постійно зростає їх суспільна небезпечність.

Науковці виділяють такі види кіберзлочинності: шахрайство з пластиковими картками; несправжні Інтернет-аукціони; шахрайство з банківськими кредитами; пошук та використання похибок в програмах; розсилка листів(спам);азартні ігри в онлайн середовищі; викуп та реєстрація доменних імен (кіберсквоттинг); крадіжка послуг (фоунфрейкинг); створення вірусів; викладення у ЗМІ неправдивих новин та інші. [1, с. 346]

Суспільна небезпечність таких злочинів, як зазначають фахівці обумовлюється наступними факторами:

- впровадження різноманітних інформаційних технологій і процесів, заснованих на використанні електронно-обчислювальних машин, у багатьох сферах людської діяльності;
- високий масштабний коефіцієнт зусиль злочинців у цій сфері;
- відносна доступність для широкого кола осіб спеціальних знань і техніки, необхідної для вчинення злочину [2, с. 304].

У чинному Кримінальному кодексі України вперше передбачено окремий самостійний розділ, який містить такі склади

злочинів – розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж», який і є такою нормативною базою. У зв'язку з цим актуальним є науковий аналіз злочинів, передбачених статтями даного розділу, і зокрема ст. 361 «Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж».

Родовим об'єктом злочинів, передбачених зазначеним розділом, є частин інформаційних відносин, засобом забезпечення яких є електронно-обчислювальні машини, системи, комп'ютерні мережі та мережі електрозв'язку. Інакше кажучи, такі злочини, посягають на певну частину інформаційних відносин – інформаційні відносини, пов'язані із застосуванням спеціальних технічних засобів. У кримінальному законі наводяться чотири види таких засобів:

- електронно-обчислювальна машина (комп'ютер);
- автоматизована система;
- комп'ютерна мережа;
- телекомунікаційна мережа;

Залежно від цих засобів інформаційні відносини, які є родовим об'єктом досліджуваних злочинів, можуть бути поділені на чотири види:

1) інформаційні відносини, засобом забезпечення яких є комп'ютери;

2) інформаційні відносини, засобом забезпечення яких є комп'ютерні системи;

3) інформаційні відносини, засобом забезпечення яких є комп'ютерні мережі;

4) інформаційні відносини, засобом забезпечення яких є мережі електрозв'язку.

Основною метою кіберзлочинця є комп'ютерна система, яка керує різноманітними процесами, і інформація, що циркулює в них. На відміну від звичайного злочинця, що діє в реальному світі, кіберзлочинець не використовує традиційну зброю – ніж і пістолет Його арсенал – інформаційна зброя, всі інструменти, що використовуються для проникнення у мережі, злому і модифікації програмного забезпечення, несанкціонованого одержання інформації або блокування роботи комп'ютерних систем. До зброї кіберзлочинця можна додати: комп'ютерні віруси, програмні закладки, різноманітні види віддалених атак, що дозволяють отримати несанкціонований доступ до комп'ютерної системи.

Об'єктивна сторона цих злочинів виявляється в активних діях. Порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них

оброблюється (ст. 363) може вчинятися шляхом злочинної бездіяльності.

Об’єктивна сторона злочинів, про які йдеться у ст. 361, ст. 362, ст. 363, ч.1 ст. 363 КК, передбачає не тільки вчинення суспільно-небезпечного діяння, а й настання суспільно небезпечних наслідків. Тож склади цих комп’ютерних злочинів є матеріальними. Склади злочинів, зазначених у ч.1 ст. 361 і ч. 2 ст.361 КК України, сформульовано законодавцем як формальні.

Говорячи про предмет даних злочинів, необхідно зазначити, що окремі автори, ймовірно, виходячи їх назви розділу 16 КК України, до їх переліку відносять комп'ютерну інформацію, віруси, відповідні програмні і технічні засоби, а також ЕОМ, комп'ютерні мережі, носії комп'ютерної інформації [3, с. 385]. Доречно погодитись із пропозицією вчених щодо розширення вчення про предмет злочинів із урахуванням сучасних тенденцій розвитку суспільних відносин та інформаційного суспільства. Відповідно ,предметом даних злочинів, у першу чергу, буде комп'ютерна інформація, а також шкідливі програмні і технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ, комп'ютерних мереж чи мереж електрозв'язку.

Суб’єкт цих злочинів – загальний (фізична осудна особа 16 років). У деяких випадках суб’єкт може бути спеціальний – особа, що має право доступу до інформації, яка обробляється в ЕОМ, автоматизованих системах, комп’ютерних мережах або зберігається на носіях такої інформації (ст. 362), або особа, що відповідає за експлуатацію ЕОМ, автоматизованих систем, комп’ютерних мереж чи мереж електрозв'язку (ст. 363).

Що стосується суб'єктивної сторони цих злочинів, то вона характеризується переважно умисною виною. Злочин, передбачений ст. 363 КК України, має необережну форму вини, що визначається характером ставлення винного до наслідків. Власне ж дія (бездіяльність) при порушенні правил експлуатації ЕОМ може бути як умисною, так і вчиненою з необережності. Створення шкідливих програмних або технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ (комп’ютерів), автоматизованих систем, комп’ютерних мереж або мереж електрозв’язку є злочинними за умови, коли ці дії вчинено з метою використання, розповсюдження чи збуту таких засобів (ч. 1 ст. 361 КК України). В інших злочинах мотив і мета можуть бути різними – корисливість, хуліганство, помста, заздрість, підрив репутації, приховування іншого злочину тощо.

Отже, можна зробити висновок що жодна держава сьогодні не здатна самостійно протистояти цьому злу. Нагальною є потреба активізації міжнародного співробітництва в сфері комп'ютерних технологій і захисту комп'ютерної інформації. Чільне місце в такому

співробітництві, безумовно посідають міжнародно-правові механізми регулювання. Але, зважаючи на те, що в сучасних умовах значна частка засобів боротьби з кіберзлочинами, як і з іншими злочинами міжнародного характеру, належить до внутрішньої компетенції кожної окремої держави, необхідно паралельно розвивати й національне законодавство спрямоване на боротьбу з комп'ютерними злочинами, узгоджуючи його з міжнародними нормами права та спираючись на існуючий позитивний досвід.

Список використаних джерел:

1. Часопис Київського університету права. – № 4 // Київ, 2010. – 346-349 с.

2. Азаров Д.С. Злочини у сфері комп’ютерної інформації (кримінально-правове дослідження): Монографія // Київ, 2007. – 304 с.

3. М.І. Бажанов, Ю.В. Баулін, В.Я. Тацій, В.В. Кримінальне право України: Особлива частина: Підручик для студентів юрид. спец. вищ. закладів освіти // Київ, 2002. – 385 с.