Овчинникова О. В.
студентка 5-го курсу факультету соціології та права КНТУУ «КПІ»
Науковий керівник: Павленко І.В.,
к.ю.н, доцент кафедри публічного права НТУУ «КПІ»

ЗЛОЧИНИ В СФЕРІ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ: ПРОБЛЕМНІ АСПЕКТИ КОЛА ІХ ВИЗНАЧЕННЯ ТА КВАЛІФІКАЦІЇ

В наш час Україна, перебуваючи в стані постійного розвитку, проводить політику реформування багатьох сфер суспільних відносин, в тому числі й правових. Починаючи з 2000-х років активно «будуються» та розвиваються нові галузі права, вдосконалюються вже існуючі, а також проходить перебудова органів державної влади та системи всієї державної влади.

Комп'ютерні технології «беруть участь» у всіх сферах сучасного суспільства – комунікації, торгівля, банківські і біржові операції та багато чого іншого.

Отже, стрімкий розвиток інформатизації та входження України в єдиний інформаційний простір дає можливість використовувати комп'ютерні технології з корисливих мотивів, що становить під загрозу окремо громадян України, так і інформаційну безпеку держави взагалі.

Злочини в сфері комп'ютерних технологій називають ще кіберзлочинами. Це поняття закріпилося у Конвенції Ради Європи про кіберзлочинність в 2001 році. Україна ратифікувала цю конвенцію у 2005 року.

Кіберзлочинність - це поняття, яке охоплює комп'ютерну злочинність та інші зазіхання, де комп'ютер є знаряддям або способом злочину проти власності, авторських прав, громадської безпеки тощо.

Регламентація інформаційно-правових відносин в державі передбачена законом, а її порушення карається у встановленому Кримінальним та Кримінальним процесуальним кодексами порядку. Слід сказати, що з початку 90-х років починається широке зростання злочинів в сфері комп'ютерних технологій, пов'язаних із започаткуванням комп'ютерно-обчислювальних та електронних засобів у державі.

Дана група злочинів включена в XVI розділ Кримінального кодексу України та містить 6 статей, в яких охарактеризовані такі види злочинів в сфері комп'ютерних технологій:

1. несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК);
2. створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361^1 КК);
3. несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^2 КК);
4. несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362);
5. порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК);
6. перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363^1 КК).

Але слід звернути увагу на те, що видів кіберзлочинів, з урахуванням високого розвитку комп'ютерних технологій, набагато більше. З'являються нові засоби та прилади, за допомогою яких вчиняються злочини.

Дуже часто з використанням комп'ютерних технологій вчиняються такі злочини: шахрайство з пластиковими картками;несправжні Інтернет аукціони; шахрайство з банківськими кредитами; азартні ігри в он-лайн середовищі; викуп та реєстрація доменних імен; крадіжка послуг;створення вірусів;крадіжка інформації та особистих даних; викрадення у електронних ЗМІ неправдивих новин.

У наш час, закони повинні відповідати вимогам, що пред’являються сучасним рівнем розвитку технологій.

Також слід приділити увагу матеріально-технічній базі. Для правильної кваліфікації злочину, розслідування потрібен достатньо високий рівень спеціальних знань, рекомендацій і роз’яснень по розслідуванню злочинів у сфері комп’ютерних технологій, судова практика по кіберзлочинності. На жаль, в Україні дуже мало фахівців, які здатні правильно кваліфікувати злочини в сфері кіберзлочинності, вислідити правопорушника і мати доказову базу для притягнення його до кримінальної відповідальності. Україні потрібно вдосконалити систему підготовки співробітників правоохоронних органів: надати потрібний об’єм знань та вмінь в сфері комп’ютерних технологій, рекомендації з чіткими діями боротьби з кіберзлочинністю, зробити узагальнення судової практики з урахуванням міжнародного досвіду.

Список використаних джерел:

1. Кримінальний кодекс України від 5 квітня 2001 року.
2. Науково-практичний коментар Кримінального кодексу України / за ред. М.І. Мельника, М.І. Хавронюка. – 4–те вид., перероблене та доповнене – К.: Юридична думка, 2007. – 1184 с.
3. Как бороться с киберпреступностью будет решать управление МВД / [Електронний ресурс]. - Режим доступу : http://jurliga.ligazakon.ua/print_news/ type_news/82911.htm.