

КОМП'ЮТЕРНА ЗЛОЧИННІСТЬ: РИЗИКИ СЬОГОДЕННЯ

Юдкова Ксенія Володимирівна

студентка 5-го курсу факультету соціології та права НТУУ «КПІ»

Науковий керівник:

Чепульченко Т. О.

Зав. кафедри теорії права і держави НТУУ «КПІ»

к. ю. н., доцент

Кінець ХХ – початок ХХІ століття став відправним моментом в розвитку інформаційних технологій. Встановити зв'язок за лічені секунди з будь-якою точкою планети видається можливим для кожного користувача Всесвітньої мережі. Уявити життя без Інтернету, без комп'ютерів сучасній людині майже неможливо. Новітні технології впроваджені в більшості галузей суспільного життя.

Але такий технічний прогрес не виключає людського фактору. На жаль, злочинність існує на будь-якому рівні, в будь-якій суспільній системі.

Насамперед слід дати визначення поняттю комп'ютерної злочинності або кіберзлочинності. Якщо звернутися до історії, то вперше поняття «комп'ютерного» злочину було сформульовано у 1979 році на Конференції асоціації адвокатів у м. Далласі (США), де були запропоновані кілька формулювань, які розглядали комп'ютерну злочинність в трьох розрізах. По-перше, використання комп'ютерів з корисливих мотивів з метою отримання матеріальних благ. По-друге, пошкодження систем математичного забезпечення та програм і інформації, що вони обробляють. По-третє, порушення зв'язку в комп'ютерних мережах та мережах локального користування.

Якщо ж дати сукупне визначення кіберзлочинності з огляду на національне законодавство України, то під комп'ютерною злочинністю ми маємо розуміти сукупність злочинів, які вчиняються суб'єктами злочину з використанням комп'ютерів, комп'ютерних технологій і систем, предметом посягання яких виступає інформація, бази даних, системні відомості та комп'ютерні програми всіх типів, при чому комп'ютер виступає засобом або знаряддям вчинення злочину.

Кримінальний кодекс України містить цілий розділ, присвячений злочинам, що вчиняються в кіберпросторі. При цьому, реально діючого механізму виявлення та доказування злочинів, що передбачають диспозиції вказаних статей в Україні наразі не існує.

Не дивлячись на достатню наукову розробленість та велику кількість інформації про такі злочини, далеко не всі взагалі знають про таке явище.

Відповідно до даних, які надає Олександр Соніс у своїй науковій статті, станом на 2004р. 55% опитаних респондентів не мають про ці категорії ані найменшого поняття, а 39% - лише частково знайомі з криміналістичним аспектом комп'ютерної діяльності з ненаукових джерел [1].

Наприклад, у США, за даними Інтерполу, за 2009р. 98,7% опитаних американців добре розуміли небезпечність існування кіберзлочинності [2].

Кіберзлочинність сьогодні набуває багатоманітності форм і виражень: хакінг і кракінг (написання шкідливих програм і злом систем захисту програмного забезпечення); порушення авторських прав; крадіжка чужих персональних даних; крадіжка номерів кредитних карт і банківських рахунків; відмивання отриманих злочинним шляхом коштів через Інтернет; кібершахрайство, у тому числі шахрайство на інтернет-аукціонах; спам.

На симпозіумі ООН по проблемах злочинів, пов'язаних з комп'ютерами і комп'ютерними мережами, кіберзлочини розглядалися у вузькому (на регіональному рівні) та широкому (на міжнародному рівні) сенсі [3]. Таке розподілення пов'язане з високим ризиком настання негативних наслідків загальнонаціонального та міжнародного масштабу, спричинених протиправними діяннями суб'єктів злочину у сфері «віртуальної дійсності».

На сьогодні комп'ютерна злочинність набула високої розповсюдженості.

В Україні, приріст кіберзлочинів становить 13—15 % щорічно [4]. При цьому вони зростають не тільки кількісно — зростає їхня складність, збільшується рівень антисоціальної спрямованості.

Основним фактором, який впливає на кількість скоєних злочинів у конкретно взятій країні, а також у світі в цілому є, згідно з думкою багатьох

фахівців, ступінь проникнення комп'ютерних технологій в усі сфери суспільного життя.

Окрім негативних чинників історичного розвитку суспільства в період науково-технічної революції, існує і ряд інших, не менш важливих, таких, що також роблять істотний вплив на розвиток нових форм злочинності. До них, зокрема можна віднести:

1) часткову втрату державним апаратом функцій повного управління суспільством і державою;

2) суперечність і недосконалість законодавчої бази;

3) відсутність або недостатнє правове регулювання громадських стосунків, що формуються у сфері інформаційних технологій;

4) недостатня правова врегульованість інших громадських відносин, що є одним з основних чинників існування соціально-економічних причин злочинності у сфері комп'ютерно-інформаційних технологій.

Кіберзлочинність – явище глобальне, міжнаціональне і прогресуюче. І його попередження вимагає від держави дуже швидкої реакції, на що певні країни (на жаль, Україна в тому числі) просто не здатні.

Спроможність держави здійснювати ефективну профілактику комп'ютерної злочинності залежить від багатьох умов: це і соціально-економічний розвиток, науково-технічний прогрес, впровадження новітніх технологій, нормальна діяльність правоохоронних органів, освітянська діяльність держави, а також суб'єктивні особливості окремих осіб.

Комп'ютерна злочинність вимагає міжнародної реакції. І, притримуючись всесвітніх програм, спираючись на досвід інших країн, розвиваючи науку і поліпшуючи економіку, Україна має всі шанси ефективно боротися з цим негативним явищем.

Список використаних джерел

1. Криминалистическая характеристика компьютерных преступлений [Електронний ресурс]. Режим доступу: 01.04.2004 <http://www.crime-research.ru/articles/Sonis0503/>

2. Офіційний сайт Інтернаціональної поліції [Електронний ресурс].
Режим доступу: <http://www.interpol.int/>
3. Матеріали офіційного сайту ООН [Електронний ресурс]. Режим доступу: <http://www.un.org/ru/>
4. Матеріали Прес-центру СБУ [Електронний ресурс]. Режим доступу: http://www.sbu.gov.ua/sbu/control/uk/publish/article?art_id=90507&cat_id=39005