ЛІТЕРАТУРА

1. Гаврилюк Д.В. Евтаназія в Україні: бути чи ні? // Права людини як критерій морального виміру політики і державної влади: зб. тез доповідей за матеріалами міжвузівських студентських наукових читань, присвячених 57-й річниці прийняття Загальної декларації прав людини (8 грудня 2005 року) / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». – Суми, 2006. – С.34-36.
2. Основи законодавства України про охорону здоров'я від 19 листопада 1992 р. // Відомості Верховної Ради України. – 1993. - №4. – Ст. 19.
3. Стеценко С.Г., Стеценко В.Ю., Сенюта І.Я. Медичне право України: Підручник / За заг. ред. д.ю.н., проф. С.Г. Стеценка. - К.: Всеукраїнська асоціація видавців «Правова єдність», 2008. - 507 с.
4. Цивільний кодекс України: Закон України від 16 січня 2003 року // Офіційний вісник України. – 2003. - №11. – Ст. 461.

Юзіков Георгій Станіславич
студент 3 курсу юридичного факультету
Дніпропетровського національного університету імені Олеся Гончара
м.Дніпропетровськ
Науковий керівник: Юзікова Н.С.
кандидат юридичних наук, доцент

ХАРАКТЕРИСТИКА ОЗНАК ЗЛОЧИНІВ У СФЕРІ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ

Для України "комп'ютерна" злочинність є відносно новим видом злочину, на відміну від багатьох інших (більш розвинутих) країн.

Так, вперше злочин з використанням ЕОМ було зареєстровано у США ще у 1969 р., коли Альфонсе Конфесоре постав перед американським судом за вчинення злочину, який спричинив шкоду на суму 620 тис. дол. Звісно, що на цьому історія "комп'ютерних" злочинів не закінчується. Майже кожен рік після цього були «гучні» пограбування які відбувалися за допомогою використання ЕОМ. У 1984 р. – з'явився перший комп'ютерний вірус.

У 1985 р., коли депутати Верховної Ради СРСР ще голосували, піднімаючи руки, у Конгресі США за допомогою вірусу була виведеназладу електронна система голосування.І далі:1989 р.–американський студент блокує 6000 ЕОМ Пентагона; 1992 р. – порушена робота реакторів Ігналінської АЕС (Литва).

На конференції країн Великої вісімки щодо проблем кіберзлочинності, яка проходила у жовтні 2000 року, міністр закордонних справ Німеччини Йошка Фішер відзначив, що збитки від кіберзлочинів сягають 100 мільярдам німецьких марок ($ 45 млрд.) щорічно. А останні роки діїкіберзлочиннцівобчислюються у сотніміліардівєвро.

Практично кожний розділ Особливої частини КК України містить норми про відповідальність за злочини, які можуть вчинятися з безпосереднім використанням комп'ютерної інформації. Це, зокрема, і розділ II "Злочини проти життя та здоров'я особи". Наприклад, в 2000 р. у США було зареєстроване перше вбивство, на замовлення, вчинене з використанням комп'ютерних технологій. Жертвою злочину став відомий бізнесмен, який знаходився на апараті штучного життєзабезпечення в одній із медичних клінік. Невідомий злочинець розробив спеціальну комп'ютерну програму, за допомогою використання мережі Інтернет пошкодив програмне забезпечення того комп'ютера, який контролював роботу системи життєзабезпечення. Внаслідок цих дій відбувся збій ПК і хворий помер.

Важко уявити наслідки незаконного втручання каналами Інтернету у роботу комп'ютерних та телекомунікаційних мереж оборонного призначення, медицини, керування наземним та повітряним транспортом тощо.

У Стокгольмі оголошено розшук людини, яку називають космічним шпигуном. Він зламав захист таємної дослідницької лабораторії військово-морського флоту США у Вашингтоні і дістав доступ до електронної програми OS/COMET, яку використовують, зокрема, для керування польотами ракет, супутників та космічних кораблів. Винний, як згодом з'ясовувалося, обрав вдалий для зламу програми час – 21 год. 30 хв. 24 грудня 2000 р., коли співробітники лабораторії вже роз'їхалися по домівках і святкували Різдво. 27 грудня служба безпеки помітила негаразди у роботі комп'ютерної системи і одразу ж її заблокувала, але було запізно..

Злочини у сфері комп'ютерної інформації можуть вчинятися і без використання глобальної комп'ютерної мережі Інтернет. Ці посягання часто здійснюються за допомогою локальних комп'ютерних мереж або при безпосередній роботі з комп'ютером. Однак використання Інтернету притаманне найбільш небезпечним злочинам у сфері комп'ютерної інформації.

Основною метою наукової публікації виступає характеристика об'єктивних та суб'єктивних ознак злочинів у сфері комп'ютерної інформації.

В теоретичному аспекті основним безпосереднім об'єктом сфері комп'ютерної інформації, на нашу думку, необхідно вважати окремо взяті відносини у сфері комп'ютерної інформації, що виникли та існують з приводу здійснення певною особою (особами) інформаційної діяльності щодо комп'ютерної інформації, і яким заподіяна шкода даним конкретним злочином або які поставлені ним під загрозу заподіяння шкоди.

Додатковим безпосереднім об'єктом злочинів, у сфері комп'ютерної інформації, на нашу думку, є відносини власності. Всі аналізовані статті спрямовані, зокрема, на захист права власності щодо комп'ютерної інформації від її протиправного перекручення, знищення, викрадення, привласнення, вимагання, заволодіння шляхом шахрайства або зловживання службовим становищем. Суспільнимвідносинамвласностізавжди буде заподіяно шкоду, оскількиінформаціязавждиперебуваєу чиїсьвласності.

Факультативним безпосереднім об'єктом аналізованих злочинів можуть виступати будь-які суспільні відносини, в залежності від того, в якій саме сфері суспільного життя використовується комп'ютерна інформація (за умови, що такі відносини не охороняються окремою кримінально-правовою нормою і відповідне посягання не утворює ще одного самостійного складу злочину). Так, при втручанні в роботу автоматизованих ЕОМ, що потягло знищення комп'ютерної інформації, наприклад, про викрадену зброю, номерні речі, автомобілі, яка міститься в оперативно-розшукових банках даних органів внутрішніх справ (АБД "Центр", АІС "Угон"), заподіюється шкода не лише відносинам у сфері комп'ютерної інформації, а й відносинам у сфері правоохоронної діяльності.

Розглядаючи предмет злочинівусферікомп'ютерноїінформації, необхідновраховуватитаке: все, щоможнарозглядати в якості предмета цихзлочинів, потрібноподілити на двічастини.

До першої частини належить носії комп'ютерної інформації (ст. 361, 363^1).

Друга група об'єднує насамперед комп'ютерну інформацію (ст. 361, 363^1, 363^2, 362, 363), а також шкідливі програмні чи технічні засоби (ст. 361^1) як особливий вид, форма існування комп'ютерної інформації.

Комп'ютерну інформацію, на нашу думку, необхідно розглядати у двох аспектах: 1) інформація як відомості про оточуючий світ та процеси, які в ньому відбуваються; 2) інформація як дані, сукупність символів, кодів, сигналів, команд

тощо, які знаходять свій вираз у різного роду комп'ютерних програмах, що забезпечують функціонування та керування комп'ютером.

У навчальній та науковій літературі об'єктивна сторона складу злочину розглядається як сукупність ознак, що характеризують зовнішній прояв злочину. До таких ознак традиційно відносять суспільно небезпечне діяння, суспільно небезпечні наслідки, причинний зв'язок між діянням та суспільно-небезпечними наслідками, а також місце, час, обстановку, спосіб, засоби та знаряддя вчинення злочину.

Більшість злочинів вчиняються виключно в активній формі (ст. 361, 361^1; 361^2; 362, 363^1), а діяння передбачене ст. 363 - посягання може вчинятися як в активній формі, так і шляхом бездіяльності.

Суб'єкт злочину, передбаченого ст. 361 КК України, а також викрадення, вимагання комп'ютерної інформації та заволодіння нею шляхом шахрайства (ст. 362 КК України), є загальним.

Суб'єктомзлочину, передбаченого ст. 363 КК України, може бути виключно особа, яка відповідає за експлуатаціюавтоматизованих ЕОМ, їх систем чикомп'ютерних мереж.

У нормах ст. 361 – 363 КК Українивідсутняпрямавказівка на те, з якою формою вини може бути вчиненененесанкціонованевтручання у роботу ЕОМ, їх систем чикомп'ютерних мереж (ст. 361 КК України). Протезміст самого поняття "втручання" обумовлюєвисновок: цейзлочиннеобхідновважатиумисним. Тільки нормою ст. 363^1 КК чіткопередбаченоумисну форму вини.

Єдиним злочином у сферікомп'ютерноїінформації, якийможе бути вчинений через необережність, є порушення правил експлуатації автоматизованих електронно-обчислювальних систем. До такого висновку нас схиляєаналіз тексту ст. 363 КК України.

Таким чином, злочини, передбачені ст. 361, 361^1, 361^2, 362, 363^1КК України, є умисними. Порушення правил експлуатації ЕОМ, їх систем чи комп'ютерних мереж особою, яка відповідає за їх експлуатацію, якщо це спричинило викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту, є злочином, який вчиняється виключно з необережності. Те саме діяння, що потягло істотне порушення роботи таких машин, їх систем чи комп'ютерних мереж, а також незаконне копіювання комп'ютерної інформації, може вчинятися і умисно, і через необережність.

Мотив і мета не охоплюються складами злочинів, передбачених ст. 361 – 363^1 КК України. Протекорисливий мотив є обов'язковоюознакоюшахрайства, вчиненого шляхом незаконнихоперацій з використанням ЕОМ (ч. 3 ст. 190 КК України).

Злочинність у сфері комп'ютерної інформації, яка є відносно новим соціальним явищем для нашої країни, набула значного розповсюдження і має тенденції до стрімкого зростання. Виходячи з того, що в Україні зареєстровано непоодинокі випадки вчинення відповідних посягань, які в основному спричиняють значну шкоду, чи потенційно можуть її спричинити важливого значення набуває правильна кваліфікація цих діянь. Визначення безпосереднього об'єкту та зосередження уваги на суб'єктивних ознаках дасть можливість уникнути помилок при застосуванні закону про кримінальну відповідальність та при призначенні відповідної адекватної міри покарання.

Бадирко Владислав Юрійович
курсант 3 курсу факультету міліції громадської безпеки Дніпропетровського державного університету