Міністерство науки і освіти України   
Київський національний університет внутрішніх справ

**Курсова робота**

**З дисципліни: «Кримінальне право України»**

Варіант 10

Виконала: студенка 4-го КА-курсу,

1 гр, заочної ф.н.,

Бондар Д.Г.

Київ 2010

**ЗМІСТ**

ВСТУП

[Розділ 1. Проблема злочинів несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів)](#_Toc268549053)

Розділ 2. Кримінально-правова характеристика несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

[Розділ 3. Приклади зі слідчої та судової практики](#_Toc268549055)

ЗАДАЧІ

[ВИСНОВКИ](#_Toc268549057)

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

**ВСТУП**

Актуальність теми дослідження. Інформаційний розвиток суспільства та запровадження на державному рівні в Україні використання мережі Internet та інших комп’ютерних систем в усіх сферах суспільного життя, поряд із позитивними здобутками, супроводжується і негативними явищами. Особливу занепокоєність викликає збільшення кількості злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), комп’ютерних систем та мереж, як в світі, так і в Україні, оскільки такі злочини не лише гальмують позитивні тенденції розвитку, а й завдають шкоди суспільству, державі, суб’єктам інформаційних відносин в усіх сферах господарювання та окремим громадянам.

Велику небезпеку являє собою поява нових форм злочинної діяльності, пов’язаних з використанням високих технологій, які раніше не були відомі. З такими проявами поки що досить складно вести ефективну боротьбу як з точки зору кримінального переслідування, так і застосування організаційно-управлінських і кримінологічних заходів з метою їх попередження. До таких злочинних посягань слід віднести умисне втручання в роботу автоматизованих систем, що призвело до перекручення чи знищення комп’ютерної інформації або носіїв інформації, чи розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручення або знищення інформації чи то носіїв інформації, кримінальна відповідальність за які в Україні була встановлена Законом України “Про внесення змін та доповнень до Кримінального кодексу України” від 20 жовтня 1994 р., яким КК України 1960 р. було доповнено статтею 1981 “Порушення роботи автоматизованих систем”. Чинний КК України також передбачив відповідальність за вчинення таких суспільно-небезпечних діянь у статті 361 “Незаконне втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж”, в ч. 1 якої передбачена відповідальність за “незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп’ютерних мереж, що призвело до перекручення чи знищення комп’ютерної інформації або носіїв такої інформації, а також розповсюдження комп’ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в ці машини, системи чи комп’ютерні мережі і здатних спричинити перекручення або знищення комп’ютерної інформації чи носіїв такої інформації”.

Попри зростаючу кількість наукових досліджень злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), їх систем та комп’ютерних мереж, вказані кримінально карані діяння залишилися недостатньо вивченими на рівні взаємопов’язаного й поглибленого аналізу всіх ознак та елементів складу злочину, передбаченого ст. 361 КК України. До останнього часу питання кримінально-правової характеристики названих злочинів розглядалися здебільшого на рівні окремих розділів підручників з Особливої частини кримінального права та коментарів КК України. Протягом останнього часу М.В. Карчевським було захищене дисертаційне дослідження з вказаної проблематики, а також захищене дисертаційне дослідження Д.С.Азаровим, присвячене характеристиці Розділу ХVI КК України в цілому. Наявність таких досліджень, а також неоднозначність підходів їх авторів до вирішення основних проблемних питань свідчить про значну увагу науковців щодо проблем кримінально-правової характеристики злочину, передбаченого ст. 361 КК України. До того ж неможливо не враховувати відсутність відповідних статистичних даних щодо порушення та розгляду кримінальних справ за ознаками злочину, передбаченого ст. 361 КК України, що свідчить, очевидно, про високий ступінь латентності вказаних діянь, на що звертається увага дослідниками питань боротьби з такими злочинами.

Проте факт незначної кількості порушення та розглянутих судами кримінальних справ даної категорії ні в якому разі не може служити підставою для неуважного ставлення до них, у тому числі на рівні наукових досліджень, особливо з урахуванням їх високої латентності.

Необхідно зазначити, що теоретичною базою послужили фундаментальні наукові положення загальної теорії кримінального права, а також праці як вітчизняних фахівців із проблеми дослідження злочинів в сфері використання електронно-обчислювальних машин, їх систем та комп’ютерних мереж, так і науковців колишнього СРСР, Російської Федерації та США, зокрема П.П. Андрушка, Ю.М. Батуріна, П.Д. Біленчука, М.С. Вертузаєва, В.Б. Вєхова, О.Г. Волеводза, В.Д. Гавловського, В.О. Голубєва, В.Г. Гончаренка, М.В. Гуцалюка, А.М. Жодзишського, Р.А. Калюжного, Ч. Кауфмана, О.І. Котляревського, В.В. Кузнєцова, В.Г. Лукашевича, В.М. Машукова, А.А. Музики, П.М. Пака, М.І. Панова, Р. Перлман, А.М. Ришелюка, Б.В. Романюка, М. Спесінера, О.П. Снігерьова, В.П. Хорста, О.М. Юрченка та багатьох інших.

Для розробки теми курсової роботи та вирішення поставлених завдань також широко використовувалися наукові роботи з загальної теорії держави і права, конституційного, кримінально-процесуального, цивільного та інших галузей права, а також з інформатики.

Актуальність боротьби з вказаними злочинами, неоднозначність підходів та висновків наукових досліджень щодо змісту ознак складу злочину, передбаченого ст. 361 КК України, та необхідність створення відповідної світовим вимогам належної вітчизняної правової бази в цій області й обумовили вибір теми цього дослідження.

Основна мета роботи полягає у комплексному аналізі об’єктивних і суб’єктивних ознак складу злочину, передбаченого ст. 361 КК України, формулюванні пропозицій щодо вдосконалення кримінального законодавства та рекомендацій з питань правильної кваліфікації досліджуваного складу злочину, відмежування його від суміжних складів та кваліфікації його за сукупністю з іншими злочинами.

Відповідно до поставленої мети вирішуються такі основні завдання:

* визначення та узагальнення чинників, що обумовлюють кримінальну відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж;
* обґрунтування необхідності виокремлення юридичних складів злочинів, які визначені в диспозиції ст. 361 КК України як альтернативні діяння об’єктивної сторони передбаченого нею складу злочину;
* з’ясування сутності та змісту об’єктивних та суб’єктивних ознак складів таких злочинів;
* дослідження і характеристика особливостей видів кваліфікованого складу таких злочинів; визначення критеріїв відмежування несанкціонованого доступу до комп’ютерної інформації та умисного
* розповсюдження шкідливих комп’ютерних програм від суміжних складів злочинів; визначення особливостей кваліфікації вказаних діянь у сукупності з іншими злочинами;
* формулювання на підставі проведеного аналізу пропозицій щодо вдосконалення чинного кримінального законодавства, яким регламентується відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж.

Об’єктом дослідження є проблеми кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), їх систем та комп’ютерних мереж.

Предметом дослідження є норми кримінального законодавства, що передбачають відповідальність за злочини в сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж.

Методи дослідження, які використовувалися в процесі здійснення дослідження: діалектичний метод, системно-структурний та функціональний методи, історико-правовий метод, порівняльно-правовий і догматичний методи.

**Розділ 1. Проблема злочинів несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів) , автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку**

На сучасному етапі розвитку суспільство стає все більше залежним від роботи комп’ютерних систем для автоматичної обробки інформації. Це стосується різних сфер діяльності людини. Усі найважливіші функції, так чи інакше, здійснюються з використанням комп’ютерів, автоматизованих систем (далі — АС) та комп’ютерних мереж і мереж електрозв’язку.

Завдяки удосконаленню комп’ютерних систем з’являються нові можливості для вчинення невідомих раніше правопорушень, а також традиційних злочинів новими засобами. Останнім часом в Україні наявна стійка тенденція до збільшення кількості злочинів, учинених у сфері використання електронно-обчислювальних машин (комп’ютерів; далі — ЕОМ), АС та комп’ютерних мереж і мереж електрозв’язку (комп’ютерних злочинів) [22, с.45].

Комп’ютерна злочинність — це особливий вид злочинів, пов’язаних із незаконним використанням сучасних інформаційних технологій і засобів комп’ютерної техніки. В їх основі можуть бути політичні, хуліганські, корисливі й інші мотиви. Це зумовлює необхідність розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності.

Інформаційні відносини, тобто відносини, що виникають при одержанні, використанні, поширенні та зберіганні інформації, регулюються положеннями Конституції України, законами від 2 жовтня 1992 р. № 2657-ХІІ «Про інформацію», вiд 25 червня 1993 р. № 3322-XII «Про науково-технічну інформацію», від 18 листопада 2003 р. № 1280-ІV «Про телекомунікації», від 5 липня 1994 р. № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах» (в редакції Закону від 31 травня 2005 р. № 2594-ІV), а також низкою підзаконних актів, зокрема Положенням про технічний захист інформації в Україні (затверджене Указом Президента України від 27 вересня 1999 р. № 1229/99) та ін.

Згідно з чинним законодавством України кримінальну відповідальність за злочини у сфері використання ЕОМ, АС та комп’ютерних мереж і мереж електрозв’язку передбачено у розд. XVI Кримінального кодексу України (далі — КК).

За даними Державної судової адміністрації України (далі — ДСА), на розгляді в місцевих та апеляційних судах у 2009 р. перебувало 156 (138) 1 кримінальних справ про злочини, відповідальність за які передбачено статтями 361-3631 КК; це на 13 % більше, ніж у 2008 р. Усього за 2009 р. було розглянуто 112 (114) справ, що на 1,8% менше, із них з постановленням вироку — 60 (65) справ, або 53,6% (57%) від кількості розглянутих.

Відповідно до вироків, що набрали законної сили, у 2009 р. було засуджено за статтями 361-3631 КК 57 (60) осіб, що на 5% менше, ніж у 2008 р. Із них за ст. 361 КК — 43 особи, або 75,4% від кількості осіб, засуджених за ці злочини; за ст. 3611 КК — три особи, або 5,3%; за ст. 3612 КК — чотири особи, або 7%; за ст. 362 КК — сім осіб, або 12,3 %. У 2008 р. дані щодо засуджених за статтями 361-3631 КК у статистичних звітах ДСА постатейно не виділялися.

Найчастіше злочини, відповідальність за які передбачена у статтях 361—3631 КК, вчиняли особи у віці: від 30 до 50 років — 23 особи (20), або 40,4% (33,3%) від кількості осіб, засуджених за ці злочини; від 18 до 25 років — 18 осіб (31), або 31,6% (51,7%); від 25 до 30 років — 11 осіб (7), або 19,3 % (11,7%); від 50 до 65 років — п’ять осіб (2), або 8,8% (3,3%) [17].

До позбавлення волі засуджено всього дві особи (5), або 3,5% (8,3%) від кількості осіб, засуджених за ці злочини. Із них одну особу засуджено за ч. 2 ст. 361 КК та одну особу — за ч. 1 ст. 3612 КК.

Штраф застосовано до 16 (13) осіб, або 28,1 % (21,7 %) від кількості засуджених за ці злочини, що на 23,1 % більше, ніж у 2008 р., у тому числі за ст. 361 КК — до 13 осіб, за ст. 3611 КК — до однієї особи, за ст. 3612 КК — до однієї особи; за ст. 362 КК також застосовано штраф до однієї особи. За ст. 361 КК засуджено одну особу, до якої застосовано інші види покарання.

Звільнено від покарання з випробуванням 38 (37) осіб, або 66,7 % (61,7 %) від кількості засуджених за ці злочини, що на 2,7 % більше, ніж у 2008 р.

Кількість осіб, щодо яких справи за статтями 361—3631 КК закрито, становить 35 (35), тобто така ж, як 2008 р. Кількість осіб, справи щодо яких закрито у зв’язку: з дійовим каяттям — 8 (6) осіб; з примиренням винного з потерпілим (за ст. 361 КК) — одна особа; зі зміною обстановки — 11 (9) осіб; з передачею особи на поруки — вісім осіб (3); з амністією — сім (15) осіб, або 20% (42,9%).

Родовим об’єктом злочинів Розділу XVI КК “Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж”, окремими науковцями визнаються суспільні відносини у сфері безпеки комп’ютерної інформації і нормального функціонування електронно-обчислювальних машин (комп’ютерів), їх систем та комп’ютерних мереж.

При цьому, конкретизуючи родовий об’єкт злочинів у сфері використання електронно-обчислювальних машин, їх систем та комп’ютерних мереж, вважаємо за необхідне включити до визначення родового об’єкту Розділу XVI КК посилання на носії комп’ютерної інформації, на яких вона зосереджується.

Тому, родовим об’єктом злочинів, відповідальність за які передбачена ст.ст. 361-363 КК, доцільно вважати суспільні відносини в сфері створення умов безперебійної та стабільної роботи електронно-обчислювальних машин (комп’ютерів), їх систем і комп’ютерних мереж та забезпечення безпеки і цілісності комп’ютерної інформації та носіїв такої інформації.

Слід зауважити, що визначення безпосереднього об’єкта злочину, передбаченого статтею 361 КК, в опублікованих роботах на сьогодні фактично не дається. На нашу думку, складнощі з визначенням безпосереднього об’єкта злочину, передбаченого ст. 361 КК, виникають, насамперед, через те, що в даній нормі містяться два логічно самостійні склади злочинів: “Несанкціонований доступ до комп’ютерної інформації ” та “Умисне розповсюдження шкідливих комп’ютерних програм” [23, с.355].

Отже, щодо питання безпосереднього об’єкта досліджуваного злочину зазначимо, що, на нашу думку, доцільно відокремлювати злочинні діяння, передбачені в ст. 361 КК, і, відповідно, визначати їх безпосередні об’єкти наступним чином:

- безпосереднім об’єктом “Несанкціонованого доступу до ЕОМ, їх систем та комп’ютерних мереж, комп’ютерної інформації та (або) носіїв такої інформації” є права власника (користувача) на виключний доступ до комп’ютерних систем, який забезпечує недоторканість та цілісність належної йому комп’ютерної інформації;

- безпосереднім об’єктом злочину “Умисне розповсюдження шкідливих комп’ютерних програм” є права власника (користувача) на безпеку програмного та технічного забезпечення комп’ютерних систем, яке забезпечує цілісність комп’ютерної інформації, її носіїв та належну роботу комп’ютерних систем.

Очевидно, що таке формулювання стосується особливостей правового захисту складових права власності: володіння, користування та розпорядження. Захист права власності в Україні гарантується ст. 41 Конституції України. Як вказано в законі України “Про інформацію”, інформація в Україні є об’єктом права власності громадян, юридичних осіб та держави. Інформація може бути об’єктом права власності як у повному обсязі, так і об’єктом лише володіння, користування чи розпорядження, як складових права власності.

Отже, ми вважаємо, що:

1. Безпосереднім об’єктом юридичного складу злочину “Несанкціонований доступ до комп’ютерної інформації” є право володіння та розпорядження комп’ютерною інформацією.

2. Безпосереднім об’єктом злочину “Умисне розповсюдження шкідливих комп’ютерних програм” є права власника (користувача) на безпеку користування технічним та програмним забезпеченням а також комп’ютерною інформацією.

Предметом злочину в класичній теорії кримінального права визнаються речі матеріального світу, діючи на які особа посягає на цінності (блага), що належать суб’єктам суспільних відносин.

Підхід до визначення предмету злочинів, що посягають на безпеку використання комп’ютерних систем, в світі є неоднаковою. Так, Кримінальний кодекс штату Юта (США) під предметом таких злочинів розуміє “відчутні та невідчутні елементи, що поріднені з комп’ютерами, комп’ютерними системами та мережами” [22, с.67-68].

Стосовно визначення предмета злочину, передбаченого ст. 361 КК України, висловлено декілька точок зору.

Предмет злочину, передбаченого ст. 361 КК України, А.М.Ришелюк визначає як: «1) автоматизовані електронно-обчислювальні машини (комп’ютери, АЕОМ), у тому числі персональні; 2) їх системи; 3) комп’ютерні мережі”. В.Г. Гончаренко предмет вказаного злочину визначає, як “кілька елементів сфери електронного інформаційного забезпечення життя суспільства: електронно-обчислювальні машини (ЕОМ); програмні матеріали, що забезпечують нормальне функціонування ЕОМ; носії інформації; системи ЕОМ та комп’ютерні мережі”. На думку М.І.Панова, предметом злочину, що розглядається, є: 1) електронно-обчислювальна машина; 2) автоматизовані комп’ютерні системи (АКС); 3) комп’ютерні мережі; 4) носії комп’ютерної інформації; 5) комп’ютерна інформація. П.П. Андрушко до предмету вказаного злочину відносить:

1) автоматизовані електронно-обчислювальні машини;

2) системи АЕОМ або автоматизовані системи;

3) комп’ютерні мережі;

4) носії комп’ютерної інформації;

5) комп’ютерні віруси;

6) комп’ютерну інформацію;

7) програмні і технічні засоби, призначені для незаконного проникнення в автоматизовані електронно-обчислювальні машини, їх системи та комп’ютерні мережі.

Наведені думки щодо кола предметів злочину, передбаченого статтею 361 КК України, мають значну низку розбіжностей. При цьому, слід зауважити, що деякі фахівці не відносять до кола альтернативних предметів злочину комп’ютерну інформацію, яка прямо вказана в статті 361 КК України як предмет, на перекручення або знищення якого направлені дії злочинця. Вважаємо, що невизнання комп’ютерної інформації окремими фахівцями предметом злочину обумовлено “матеріалістичним” підходом класичної теорії кримінального права до визначення предмета злочину як певних матеріальних цінностей. В той час, комп’ютерна інформація є предметом віртуальним, тобто “умовним, фізично відсутнім, але за допомогою спеціальних методів наданим у розпорядження”.

На нашу думку, під віртуальним слід розуміти такий предмет об’єктивного світу, який створений за допомогою спеціальних методів та (або) способів, є фізично відсутнім, але має зовнішнє представлення, або може набути такого представлення за допомогою спеціальних методів або способів впливу.

Під предметом злочину доцільно розуміти речі або інші явища об’єктивного світу, як матеріальні, так і віртуальні, з певним впливом на які кримінальний закон пов’язує наявність у діянні особи складу конкретного злочину.

У відповідності з законодавчим визначенням норми “незаконне втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж”, передбаченої ст. 361 КК, альтернативними предметами даного злочину, на нашу думку, є: електронно обчислювальні машини, їх системи та комп’ютерні мережі, комп’ютерна інформація та носії комп’ютерної інформації.

У п.7.3 ДСТУ “Автоматизовані системи. Терміни та визначення”, під машиною обчислювальною цифровою (синонім “електронно-обчислювальна машина” – Н.Р.) розуміється сукупність технічних засобів та системного програмного забезпечення, яка створює можливість обробки інформації та отримання результату в необхідній формі.

На нашу думку, електронно-обчислювальна машина (комп’ютер) - це комплекс технічних і програмних засобів, призначених для автоматичної обробки інформації, яка частково керована оператором.

Під поняттям “їх системи” в контексті ст. 361 КК, на наш погляд, слід розуміти операційні системи електронно-обчислювальних машин, які забезпечують безпосередньо роботу на конкретній електронно-обчислювальній машині, а також спеціальні прикладні операційні системи, які призначені як до локальної роботи, так і для роботи в комп’ютерній мережі [12, с.56].

Так, до операційних систем електронно-обчислювальних машин належать, зокрема, такі операційні системи як Norton Commander, MS-DOS, Windows, які є пакетом програмного забезпечення для роботи на окремій електронно-обчислювальній машині, або в локальній мережі (в разі встановлення в локальній мережі мережевої версії операційної системи).

Операційні системи електронно-обчислювальних машин є складовими самих електронно-обчислювальних машин, роботу яких (загальну або специфічну) вони забезпечують.

Тому, на нашу думку, поняття “комп’ютерні системи” є значно ширшим поняття “системи електронно-обчислювальних машин”, а також понять “електронно-обчислювальні машини” та “комп’ютерні мережі”. Тобто, поняття “комп’ютерні системи” поглинає “електронно-обчислювальні машини ( комп’ютери), їх системи та комп’ютерні мережі”.

Для остаточного визначення такої необхідності проведемо аналіз наукового визначення поняття “комп’ютерна мережа”.

У популярній літературі комп’ютерною мережею визнається сукупність автономних електронно-обчислювальних машин, поєднаних лініями передачі даних для взаємного узгодження обміну інформацією.

Держстандарт України визначає комп’ютерну мережу як систему “сполучених між собою комунікаційними засобами ЕОМ різної продуктивності та конфігурації”.

Комп’ютерні мережі в межах невеликої території (підприємство, організація) зазвичай називаються локальними; мережі, які охоплюють значні простори (край, держава, континент) – глобальними. Мережа Internet має визнаватися світовою комп’ютерною мережею.

На наш погляд, комп’ютерна мережа - це сукупність територіально розмежованих електронно-обчислювальних машин і терміналів (робочих місць), поєднаних каналами зв’язку, яка забезпечує автоматизовану обробку даних і можливість обміну інформацією, а також користування загальними ресурсами [22, с.98].

Під каналами або лініями зв’язку розуміють фізичні канали або середовище зв’язку між технічними засобами інформаційної мережі.

Конвенція про кіберзлочинність, щодо визначення електронно-обчислювальних машин, їх систем та комп’ютерних мереж, вживає, як було вказано вище, узагальнююче поняття – “комп’ютерні системи”, під яким розуміє будь-який пристрій чи групу взаємопов’язаних чи суміжних пристроїв, один чи більше з яких, діючи за програмою, здійснює автоматизовану обробку даних. Виходячи з того, що Україна, як держава-учасниця Конвенції про кіберзлочинність, погодилась з прийняттям такої норми, поняття “комп’ютерні системи” може застосовуватись в Україні щодо предметів злочину, передбаченого ст. 361 КК України та в загальному розумінні сукупності електронно-обчислювальних машин, їх систем та комп’ютерних мереж.

На нашу думку, під узагальнюючим поняттям альтернативних предметів злочину передбаченого ст. 361 КК, а саме електронно-обчислювальних машин, їх систем та комп’ютерних мереж, слід вживати термін “комп’ютерні системи”, який у повному обсязі охоплює зазначені альтернативні предмети.

Істотно важливим залишається визначення поняття “комп’ютерна інформація», яке є спірним і не має єдиного визнання.

Закон України “Про інформацію” в ст. 1 визначає інформацію як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі. Однак, у переліку видів інформації, визначеного ст. 8 даного Закону, комп’ютерна інформація не згадується. Тобто, законодавець не проявляє сучасного підходу до визначення комп’ютерної інформації як одного з найпопулярніших видів інформації, що існує в світі і в Україні.

До того ж поняття «комп’ютерна інформація” не включене до деяких нормативних актів, де її присутність як предмета захисту має бути обов’язковою. Так, у Законі України “Про науково-технічну інформацію” від 25 травня 1993 року щодо розкриття поняття “науково-технічна інформація” (ст. 1), жодне з понять “комп’ютерна інформація”, “інформація в автоматизованих системах”, “інформація в комп’ютерних системах”, - не визначається.

Закон України «Про захист інформації в автоматизованих системах», визначає інформацію в автоматизованих системах як «сукупність усіх даних і програм, які використовуються в АС незалежно від засобу їх фізичного та логічного представлення». Інформація в автоматизованих системах є синонімом термінів “комп’ютерна інформація”, та “інформація в комп’ютерних системах”.

Також, необхідно вказати, що оцінювання комп’ютерної інформації виключно як сукупності (єдності) програм, даних, файлів є недоцільним, через те, що кожна програма, файл або база даних також є різновидом комп’ютерної інформації, і кримінальна відповідальність повинна наступати за порушення цілісності або руйнування хоча б одного з вказаних предметів. В іншому випадку, тобто в разі визнання предметом злочину сукупності всіх програм, баз даних та файлів в електронно-обчислювальних машинах, втрачають сенс деякі з інших важливих положень. Наприклад, визначення в якості кваліфікуючої ознаки в ч. 2 ст. 361 КК України “заподіяння істотної шкоди” стає недоцільним, тому що за ч. 1 ст. 361 КК можна буде притягнути до кримінальної відповідальності лише особу, яка спричинила тотальну шкоду комп’ютеру, тобто, коли вона руйнівно вплинула на всю сукупність програмного забезпечення і інформації, що зберігалась в електронно-обчислювальній машині. В такому випадку відсутня диференціація між поняттям “шкода” і “істотна шкода”, так як під поняття “шкода” підпадатиме виключно тотальний вплив на комп’ютерну систему – вплив на “сукупність всіх даних і програм”. Якщо суб’єктом буде завдано шкоди одній програмі, така особа, відповідно до наведених тверджень, може уникнути кримінальної відповідальності [18, с.23-24].

Крім того, відсутній практичний сенс зазначати обов'язковою ознакою комп’ютерної інформації наявність у неї спеціального захисту, якщо злочин, що посягає на цілісність інформації не сформульовано як «Несанкціонований доступ до комп’ютерної інформації”. Досить вказати, на нашу думку, на наявність авторизації інформації, тобто фіксації її приналежності певному власникові або користувачеві.

Вважаємо за необхідне зазначити, що програмне забезпечення електронно-обчислювальних машин, їх систем та комп’ютерних мереж, у відповідності з визначенням поняття “комп’ютерна інформація”, безпосередньо належить до комп’ютерної інформації.

Однак, ми вважаємо також, що в деяких випадках, наприклад, при визначенні предмета злочину “Умисне розповсюдження шкідливих комп’ютерних програм», необхідне самостійне визначення поняття «програмне забезпечення» в сукупності з «технічним забезпеченням» електронно-обчислювальних машин, їх систем та комп’ютерних мереж. Шкода технічному забезпеченню автоматизованих систем може бути завдана лише опосередковано: впливу шкідливих програмних засобів зазнає програмне забезпечення, і таке “пошкоджене” програмне забезпечення здатне завдати шкоди технічному забезпеченню електронно-обчислювальних машин, їх системам або комп’ютерним мережам.

Отже, виходячи з визначення поняття “комп’ютерна інформація”, засоби програмно-математичного захисту, а саме паролі та коди доступу до комп’ютерних систем, а також до комп’ютерної інформації та її носіїв, також слід відносити до предмета злочину, передбаченого статтею 361 КК України, через те, що вони:

1) відповідають ознакам “комп’ютерної інформації»;

2) здійснюють захисну функцію інших предметів вказаного злочину.

Захисні системи, що належать до апаратно-програмного захисту, повинні в частині програмного забезпечення тлумачитись, як різновид комп’ютерної інформації.

При цьому, поза увагою залишаються інші захисні засоби, які належать до суто апаратного захисту, та апаратно-програмні засоби в частині апаратного забезпечення.

За умови апаратного захисту, а також у випадку апаратно-програмного захисту, закладеного в самій електронно-обчислювальній машині, системі, або комп’ютерній мережі, тобто, якщо захисні пристрої вмонтовані або технічно пов’язані з електронно-обчислювальними машинами або терміналами системи чи комп’ютерної мережі, їх слід розглядати, як технічні елементи електронно-обчислювальних машин, їх систем та комп’ютерних мереж. Тобто, технічні (апаратні) засоби захисту також повинні визначатися як один з альтернативних предметів досліджуваного злочину [22, с.106].

**злочин комп'ютер мережа втручання слідчий судовий**

**Розділ 2. Кримінально-правова характеристика несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку**

Спираючись на Конвенцію Ради Європи про кіберзлочинність від 23 листопада 2001 р., слід вживати термін “комп’ютерні системи” в якості узагальнюючого (родового) поняття, що охоплює поняття “електронно-обчислювальні машини (комп’ютери)”, “системи електронно-обчислювальних машин” та “комп’ютерні мережі”. На рівні національного законодавства слід встановити відповідальність за вчинення окремих злочинів, передбачених міжнародно-правовими нормами, а також необхідним є узгодження основних положень нормативних актів, що обумовлюють інститут комп’ютерної злочинності (кіберзлочинності) [22, с.45].

Очевидно, кримінальні закони окремих країн СНД, містять надто широкий перелік злочинів, які підмінюють собою традиційні склади злочинів і провокують штучне виникнення колізій. З другого боку, кримінальні закони інших країн СНД передбачають кримінальну відповідальність за вчинення комп’ютерних злочинів однією нормою, яка, здебільшого, містить кілька логічно самостійних складів в межах однієї диспозиції. Найбільш оптимальним, є регламентація кримінальної відповідальності за незаконне втручання в роботу комп’ютерних систем в якості виділення двох самостійних юридичних складів злочинів, які передбачають кримінальну відповідальність за несанкціонований доступ до комп’ютерної інформації та за умисне розповсюдження шкідливих комп’ютерних програм.

Однією з причин неефективності норми, що передбачає кримінальну відповідальність за незаконне втручання в роботу електронно-обчислювальних машин, систем та комп’ютерних мереж, є невідповідність її міжнародним стандартам, оскільки в межах норми визначені два логічно самостійні юридичні склади злочинів, законодавчий опис ознак яких є неповним і не відповідає реаліям вчинення таких злочинних діянь. Крім того, в Україні фактично відсутні єдині підходи щодо визначення основних чинників та понять, що описують такі злочини.

У ст. 361 КК України містяться два логічно самостійні юридичні склади злочинів, які умовно можна позначити як “Несанкціонований доступ до комп’ютерної інформації” та “Умисне розповсюдження шкідливих комп’ютерних програм”.

В процесі аналізу безпосереднього об’єкту незаконного втручання в роботу електронно-обчислювальних машин, систем та комп’ютерних мереж, можна зробити висновок, що його встановлення фактично стає можливим виключно при виокремленні в самостійні юридичні склади діянь по несанкціонованому доступу до комп’ютерної інформації та по умисному розповсюдженню шкідливих комп’ютерних програм.

Безпосередній об’єкт злочину “Несанкціонований доступ до комп’ютерної інформації” можна визначити як права власника (користувача) на виключний доступ до комп’ютерних систем, який забезпечує недоторканність і цілісність комп’ютерної інформації; безпосередній об’єкт злочину “Умисне розповсюдження шкідливих комп’ютерних програм” - як права власника (користувача) на безпеку програмного і технічного оснащення комп’ютерних систем, яким забезпечується цілісність комп’ютерної інформації, її носіїв та належну роботу комп’ютерних систем.

Розенфельд Н.А. у своїй дисертаційній роботі „Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж” до переліку альтернативних предметів злочину, передбаченого ст. 361 КК України, відносить: електронно-обчислювальні машини, системи електронно-обчислювальних машин, комп’ютерні мережі, комп’ютерну інформацію (в тому числі програмно-математичні засоби її захисту), а також носії комп’ютерної інформації. В разі виокремлення в самостійні юридичні склади діянь, що являють собою незаконне вручання в роботу комп’ютерних систем, предметом злочину “Несанкціонований доступ до комп’ютерної інформації” автор визнає комп’ютерну інформацію, під якою дисертант розуміє інформацію, що зберігається на електронних носіях, або пересилається між ними, незалежно від форм її фізичного або логічного представлення, і може використовуватися, оброблятися, змінюватися за допомогою електронно-обчислювальної машини; альтернативними предметами злочину “Умисне розповсюдження шкідливих комп’ютерних програм” - комп’ютерну інформацію та її носії. Особливості форм представлення комп’ютерної інформації зумовили необхідність дослідження її як різновиду предмету, який може бути віднесений, на думку, автора до віртуального предмету, під яким розуміється такий предмет об’єктивного світу, який створений за допомогою спеціальних методів та (або) способів, є фізично відсутнім, але має зовнішнє представлення, або може набути такого представлення, за допомогою спеціальних методів або способів впливу [25, с.204].

Однією з причин необхідності виокремлення зазначених злочинів в самостійні юридичні склади є те, що склад злочину “Несанкціонований доступ до комп’ютерної інформації” є матеріальним, в той час, як склад злочину “Умисне розповсюдження шкідливих комп’ютерних програм” є формальним.

Об’єктивна сторона складу злочину “Несанкціонований доступ до комп'ютерної інформації” характеризується вчиненням активних дій по доступу до комп’ютерної інформації, що призвело до настання будь-якого з альтернативних наслідків у вигляді витікання, перекручення або знищення інформації.

Необхідним вбачається доповнення переліку ознак об’єктивної сторони складу злочину “Несанкціонований доступ до комп’ютерної інформації” наслідком у вигляді витікання комп’ютерної інформації, що, поряд з перекрученням і знищенням такої, може становити загрозу суспільним відносинам; під витіканням розуміється несанкціоноване копіювання, пересилання, або поширення комп’ютерної інформації, за умови, що в комп’ютерній системі власника (або користувача) інформація не зазнає змін.

Об’єктивну сторону складу злочину “Умисне розповсюдження шкідливих комп’ютерних програм” складають активні діяння по розповсюдженню комп’ютерного вірусу, або інших шкідливих комп’ютерних програмних засобів, які здатні спричинити перекручення або знищення комп’ютерної інформації чи її носіїв.

До факультативних ознак об’єктивної сторони злочину “Несанкціонований доступ до комп’ютерної інформації” належать знаряддя вчинення такого злочину - програмні і технічні засоби, призначені для несанкціонованого проникнення в комп’ютерні системи або для доступу до комп’ютерної інформації.

Специфічним знаряддям злочину “Умисне розповсюдження шкідливих комп’ютерних програм” є безпосередньо шкідливі комп’ютерні програми, серед яких виділяється комп’ютерний вірус, під яким автор розуміє специфічну комп’ютерну програму, яка, приєднуючись до інших файлів, здатна, непомітно для власника (користувача), імпортуватись в комп’ютерну систему, і шляхом самовідтворення здатна привести до наслідків у вигляді: знищення, блокування, зміни, автономного копіювання, відсилання небажаному адресатові тощо комп’ютерної інформації, а так само (або) спрямована на спричинення шкоди носіям комп’ютерної інформації, програмному або технічному забезпеченню комп’ютерної системи. Передбачені ж ч. 1 ст. 361 КК України програмні і технічні засоби, призначені для незаконного проникнення в комп’ютерну систему і здатні спричинити перекручення або знищення комп’ютерної інформації, автор вважає доцільним розглядати, в залежності від спрямованості застосування, як спосіб або знаряддя вчинення злочину “Умисне розповсюдження шкідливих комп’ютерних програм”.

Суб’єктом таких злочинів є фізична осудна особа, якій до вчинення злочину виповнилось шістнадцять років (загальний суб’єкт) [22, с.143].

Злочинні діяння по несанкціонованому доступу до комп’ютерної інформації характеризуються наявністю вини у формі прямого або непрямого (евентуального) умислу, в той час як діяння по умисному розповсюдженню шкідливих комп’ютерних програм можуть вчинюватись виключно з прямим умислом; обґрунтована необхідність обов’язкового встановлення факультативних ознак суб’єктивної сторони складу злочину - мотиву і мети при вчиненні діянь по незаконному втручанню в роботу комп’ютерних систем, через те, що наявність специфічних мотивів і цілей вчинення таких діянь свідчитиме про можливу сукупність з іншими злочинами.

Розглянемо окремі аспекти кваліфікованого складу злочину “Незаконне втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж”.

Поняття “істотна шкода” в частині істотності заподіяної шкоди має визнаватися оціночним, тобто питання про істотність для потерпілого шкоди, заподіяної діянням по несанкціонованому доступу до комп’ютерної інформації або по умисному розповсюдженню шкідливих комп’ютерних програм, повинне визначатися судом в кожному конкретному випадку. На думку Розенфельд Н.А. у своїй дисертаційній роботі „Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж”, шкода може визнаватися істотною, якщо вона: спричинила моральні або фізичні страждання потерпілому; спричинила значні для потерпілого збитки; спричинила інші тяжкі наслідки.

В разі виокремлення в самостійні юридичні склади злочинів “Несанкціонований доступ до комп’ютерної інформації” та “Умисне розповсюдження шкідливих комп’ютерних програм” , повторність щодо їх вчинення повинна визначатися як спеціальна. У відповідності з чинною редакцією ст. 361 КК України повторним слід вважати вчинення два або більше разів будь-якого з діянь, що містять склади злочинів, передбачені ч. 1 ст. 361 КК України. В разі виокремлення вказаних діянь в самостійні статті КК України, на думку автора, їх повторність також повинна визначатися як спеціальна.

Злочин, передбачений ч. 1 ст. 361 КК України, вважається таким, що вчинений за попередньою змовою групою осіб, якщо у його вчиненні як співвиконавці брали участь не менш як дві особи, домовленість про спільне вчинення якого було досягнуто між ними до моменту початку дій по несанкціонованому доступу до комп’ютерної інформації або по умисному розповсюдженню шкідливих комп’ютерних програм [22, с.154].

Вчинення злочину, передбаченого ч. 1 ст. 361 КК України, на замовлення, не охоплюється кваліфікованим складом, передбаченим ч. 2 ст. 361 КК України - вчинення такого злочину за попередньою змовою групою осіб”, тому ч. 2 ст. 361 КК України потребує на доповнення її альтернативним видом кваліфікованого складу - вчинення діянь, передбачених ч. 1 ст. 361 КК України, на замовлення.

Відмежування злочину “Незаконне втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж” слід проводити від суміжних складів злочинів “Викрадення, привласнення, вимагання комп’ютерної інформації або заволодіння нею шляхом шахрайства або зловживання службовим становищем”, передбаченого ст. 262 КК України, та злочину “Порушення правил експлуатації автоматизованих електронно-обчислювальних систем”, передбаченого ст. 363 КК України.

Відмежування злочину “Незаконне втручання в роботу електронно–обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж” від злочину “Викрадення, привласнення, вимагання комп’ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем” має відбуватися за ознаками об’єктивної сторони, а також за тими з ознак, які є спеціальними для даних норм. Так спеціальними ознаками, передбаченими в ст. 362 КК України є: способи розкрадання комп’ютерної інформації, привласнення, або заволодіння шляхом зловживання посадовим становищем; обов’язкова наявність у винної у привласненні комп’ютерної інформації особи ознак спеціального суб’єкта, вчинення такого злочину виключно з прямим умислом.

Відмежування злочину “Незаконне втручання в роботу електронно–обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж” від злочину “Порушення правил експлуатації автоматизованих електронно–обчислювальних систем” передбачених ст. 361 та ст. 363 КК України слід проводити за специфічними ознаками. До специфічних ознак, за якими провадиться відмежування зазначених суміжних складів, можна віднести ознаки їх суб’єктів та суб’єктивної сторони. Особливу увагу слід зосередити на тому, що наявність умислу на вчинення порушення правил експлуатації автоматизованих систем, відповідальність за яке передбачена ст. 363 КК України, може вчинюватись з метою полегшення вчинення іншого злочину, зокрема, передбаченого ст. 361 або ст. 362 КК України.

**Розділ 3. Приклади зі слідчої та судової практики**

В Україні найбільш поширеним злочином у сфері використання ЕОМ, АС та комп’ютерних мереж і мереж електрозв’язку є злочин, відповідальність за який передбачено ст. 361 КК («Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку») [8].

Об’єктом такого злочину є ЕОМ, АС, комп’ютерні мережі та мережі електрозв’язку. Об’єктом такого злочину також може бути право власності на комп’ютерну інформацію.

Для визнання факту вчинення злочину, склад якого передбачено у ст. 361 КК, суд має встановити не лише вчинення діяння, а й настання хоча б одного із зазначених в законі наслідків: витоку, втрати, підроблення, блокування інформації, спотворення процесу її обробки або порушення встановленого порядку її маршрутизації. Тобто між несанкціонованим втручанням в роботу ЕОМ, АС, комп’ютерних мереж чи мереж електрозв’язку має бути причинний зв’язок хоча б з одним із суспільно небезпечних наслідків.

Специфіка розгляду справ цієї категорії полягає у правильному розумінні термінів, визначення яких містяться у наведених вище нормативних документах.

ЕОМ розуміється як комплекс електронних технічних засобів, побудованих на основі мікропроцесорів і призначених для автоматичної обробки інформації при вирішенні обчислювальних та інформаційних завдань.

АС — це організаційно-технічні системи, в яких реалізується технологія обробки інформації з використанням технічних і програмних засобів. Зокрема, такими системами слід вважати сукупність ЕОМ, засобів зв’язку та програм, за допомогою яких ведеться документообіг, формуються, оновлюються та використовуються бази даних, накопичується та обробляється інформація. Оскільки обробка певних даних можлива і в результаті роботи одного комп’ютера, то АС — це й окремо взятий комп’ютер разом з його програмним забезпеченням.

Комп’ютерна мережа — це сукупність програмних і технічних засобів, за допомогою яких забезпечується можливість доступу з однієї ЕОМ до програмних чи технічних засобів інших ЕОМ та до інформації, що зберігається у системі іншої ЕОМ [8].

Мережа електрозв’язку — комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

Об’єктивна сторона злочину проявляється у формі несанкціонованого втручання в роботу ЕОМ, їх систем, комп’ютерних мереж чи мереж електрозв’язку, наслідком якого є: 1) витік; 2) втрата; 3) підроблення; 4) блокування інформації; 5) спотворення процесу автоматичної обробки інформації; 6) порушення встановленого порядку її маршрутизації.

Несанкціоноване втручання в роботу ЕОМ, їх систем чи комп’ютерних мереж — це проникнення до цих машин, їх систем чи мереж і вчинення дій, які змінюють режим роботи машин, їх систем чи комп’ютерних мереж або повністю чи частково припиняють їх роботу без дозволу відповідного власника або уповноваженої особи.

Несанкціонованим втручанням в роботу мереж електрозв’язку слід вважати будь-які (окрім втручання в роботу ЕОМ, їх систем чи комп’ютерних мереж, що забезпечують роботу мереж електрозв’язку) вчинені без згоди власника відповідної мережі чи службових осіб, на яких покладено забезпечення її нормальної роботи, дії, внаслідок яких припиняється (зупиняється) робота мережі електрозв’язку або відбуваються зміни режиму цієї роботи.

Комп’ютерна інформація — це текстова, графічна чи будь-яка інша інформація (дані), яка існує в електронному вигляді, зберігається на відповідних носіях і може бути створена, змінена чи використана за допомогою ЕОМ.

Способи несанкціонованого втручання (проникнення) в роботу зазначених систем і мереж у судовій практиці трапляються різні. Як засвідчили матеріали узагальнення, найчастіше вчинення дій, передбачених ст. 361 КК, відбувається з метою безкоштовного доступу до мережі Інтернет.

Наприклад, Сєвєродонецький міський суд Луганської області вироком від 7 червня 2007 р. визнав Г. винним у тому, що він, маючи достатні технічні навики роботи на комп’ютері, використовуючи останній, не санкціоновано, без дозволу провайдера ТОВ «HomeLAN» втручався в роботу його мережі під чужими мережевими реквізитами. Таке несанкціоноване втручання в роботу комп’ютерних мереж призводило до блокування надходження інформації до офіційних користувачів, унеможливлюючи їм доступ до цих мереж, вносило викривлення в процес обробки інформації, порушувало порядок її маршрутизації [8].

Дії Г. суд кваліфікував за ч. 1 ст. 361 КК і призначив йому відповідне покарання.

У ч. 2 ст. 361 КК передбачено відповідальність за такі ж самі дії, що й у ч. 1 цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду.

Оскільки вчинення цього злочину за попередньою змовою групою осіб є кваліфікуючою ознакою для ч. 2 ст. 361 КК, то в разі його вчинення за таких обставин дії винних осіб не потребують додаткової кваліфікації за ст. 28 КК. Проте в деяких випадках суди допускали помилки при кваліфікації зазначених дій.

Так, Хмельницький міськрайонний суд Хмельницької області визнав Г. та С. винними за ч. 2 ст. 28, ч. 2 ст. 361 КК і призначив їм відповідне покарання. Г. та С. вироком суду визнано винними у тому, що вони, діючи за попередньою змовою між собою, шляхом несанкціонованого втручання в роботу мереж електрозв’язку порушили встановлений порядок маршрутизації міжнародних телефонних дзвінків.

Міськрайонний суд помилково кваліфікував дії цих засуджених за ч. 2 ст. 28 КК. Виправляючи помилку, Апеляційний суд Хмельницької області ухвалою від 26 грудня 2006 р. змінив вирок суду першої інстанції, виключивши з їх обвинувачення ч. 2 ст. 28 КК.

Згідно з приміткою до ст. 361 КК, шкода у статтях 361—3631 КК вважається значною, якщо вона полягає у заподіянні матеріальних збитків, що в 100 і більше разів перевищують неоподатковуваний мінімум доходів громадян. Таким чином, значна шкода може мати і нематеріальний характер. У разі вчинення діянь, передбачених статтями 361—3631 КК, нематеріальна шкода може полягати у тимчасовому зупиненні (припиненні) роботи або іншому порушенні нормального режиму роботи певного підприємства, організації, установи, їх окремих структурних підрозділів, підриві ділової репутації громадянина чи юридичної особи, заподіянні громадянину моральної шкоди внаслідок втрати, незаконного поширення чи витоку інформації, яка є результатом його наукової чи творчої діяльності, тощо. Значна шкода нематеріального характеру є оціночним поняттям. Отже, питання про те, чи слід визнавати таку шкоду значною, вирішують органи досудового слідства, прокурор або суд з урахуванням конкретних обставин справи.

Матеріали узагальнення свідчать, що збільшилась кількість випадків, коли несанкціоноване втручання в роботу ЕОМ, АС, комп’ютерних мереж здійснювалося з корисливих мотивів з метою викрадення чи заволодіння чужим майном із заподіянням потерпілим матеріальної шкоди і було способом вчинення таких злочинів проти власності, як шахрайство (ст. 190 КК) або привласнення чи заволодіння майном шляхом зловживання службовим становищем (ст. 191 КК). У більшості випадків суди кваліфікували такі дії за сукупністю злочинів: за ст. 361 КК і тією статтею, в якій передбачено відповідальність за конкретний злочин проти власності, способом здійснення якого було несанкціоноване втручання в роботу ЕОМ, АС, комп’ютерних мереж і мереж електрозв’язку.

Наприклад, Печерський районний суд м. Києва вироком від 12 лютого 2007 р. визнав М. винним у тому, що він, працюючи провідним інженером відділу пластикових карток акціонерного комерційного «Промислово-фінансового банку», як службова особа, що виконує адміністративно-господарські функції, в 2006 р., зловживаючи своїм службовим становищем, маючи доступ до бази даних про клієнтів та їхні рахунки, що містилась у його робочому комп’ютері, діючи з метою заволодіння грошовими коштами, виконав операцію з персоналізації сторонньої картки, скопіювавши на неї інформацію одного з клієнтів банку. З використанням картки-дубліката та банкоматів М. зняв і привласнив готівкою з рахунку клієнта грошові кошти на загальну суму 65 тис. 900 грн. Зазначені дії М. суд кваліфікував за ч. 4 ст. 191 КК як заволодіння чужим майном шляхом зловживання службовим становищем, вчинене у великих розмірах [8].

Крім того, суд правильно кваліфікував дії М. ще й за сукупністю злочинів, склад яких передбачено ч. 3 ст. 362 КК, оскільки М., будучи особою, яка мала право доступу до інформації, що оброблялася на комп’ютерах та зберігалася на носіях, несанкціоновано її скопіював, що призвело до витоку інформації і заподіяло значну шкоду.

Проте в деяких випадках суди кваліфікували зазначені дії лише за тими статтями КК, в яких передбачено відповідальність за вчинення комп’ютерних злочинів.

Так, Красногвардійський районний суд м. Дніпропетровська вироком від 4 грудня 2006 р. визнав Є. винним за ч. 1 ст. 361 КК і призначив йому відповідне покарання. З матеріалів справи вбачається, що Є., діючи з корисливих мотивів, за допомогою спеціальних комп’ютерних програм створив дублікат-макет сайту компанії, яка спільно із закритим акціонерним товариством комерційним банком «ПриватБанк» (далі — ЗАТ КБ «ПриватБанк») надавала послуги з прискореного перерахування платежів за комунальні послуги і мобільний зв’язок через мережу Інтернет. У результаті такої діяльності Є. протягом певного часу викрадав грошові кошти з рахунків клієнтів ЗАТ КБ «ПриватБанк».

Оскільки Є. шляхом обману неодноразово заволодівав грошовими коштами за допомогою незаконних операцій з використанням ЕОМ, а втручання в роботу ЕОМ є способом вчинення злочину проти власності, то в цьому випадку зазначені дії потребують додаткової кваліфікації ще й за ст. 190 КК (шахрайство).

Вивчення справ про комп’ютерні злочини показало, що значна кількість їх пов’язана із несанкціонованим втручанням в роботу мереж електрозв’язку шляхом використання емуляторів — телефонних карток, що дають змогу безкоштовно здійснювати з таксофонних автоматів дзвінки в будь-якому напрямку, у тому числі за межі України. Такі дії завдають значних збитків телекомунікаційним компаніям, за рахунок яких здійснюються дзвінки у віддалені регіони; при цьому вчинювані телефонні виклики, як правило, не прослідковуються, і за них компанія не в змозі виставити рахунок користувачеві.

Наприклад, Центральний районний суд м. Сімферополя вироком від 20 вересня 2006 р. визнав С. винним за ч. 2 ст. 361 КК і призначив йому відповідне покарання. З матеріалів справи вбачається, що С., діючи повторно, з метою отримання матеріальної вигоди для здійснення безкоштовних дзвінків придбав емулятор таксофонної картки із впаяним у нього запрограмованим чіпом. Використовуючи зазначений емулятор, С. надавав послуги міжміського та міжнародного телефонного зв’язку стороннім особам, а кошти, одержані за ці послуги, привласнював. Таким чином, було здійснено 1 тис. 177 незаконних безоплатних телефонних дзвінків, у тому числі й за кордон, та завдано збитків відкритому акціонерному товариству «Укртелеком» (далі — ВАТ «Укртелеком») на суму 11 тис. 980 грн.

Згідно з висновком судово-технічної експертизи, вилучений у С. технічний пристрій є емулятором телефонної картки для несанкціонованого доступу до послуг ВАТ «Укртелеком». Емулятор таксофонної картки був виготовлений шляхом видалення електронного модуля із пластикової картки і встановлення на це місце мікропроцесора, в якому записано програмне забезпечення, що емулуює роботу електронної картки.

У цьому випадку грошові кошти у вигляді оплати за міжміські та міжнародні розмови, які мали б надійти в розпорядження власника телефонної мережі, отримував зловмисник, тому ця грошова сума є неодержаним прибутком власника. Неодержаний прибуток є предметом злочину ст. 192 КК (заподіяння майнової шкоди шляхом обману або зловживання довірою). Отже, дії С. слід було б додатково кваліфікувати ще й за ч. 1 ст. 192 КК.

Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ, АС, комп’ютерних мереж чи мереж електрозв’язку, тягне відповідальність за ст. 3611 КК. Як предмет цього злочину комп’ютерні програми (програмні засоби) мають бути шкідливими, тобто здатними забезпечити несанкціонований доступ до інформації, а також змінити, знищити, пошкодити, заблокувати інформацію — комп’ютерну чи ту, яка передається мережами електрозв’язку. Різновидом шкідливих комп’ютерних програм є комп’ютерні віруси. Їх призначення — несанкціоноване втручання в роботу ЕОМ, АС, комп’ютерних мереж чи мереж електрозв’язку. Зазначений злочин (ч. 1 ст. 3611 КК) має формальний склад, і для наявності його об’єктивної сторони не потрібне настання суспільно небезпечних наслідків.

Так, Дрогобицький міськрайонний суд Львівської області вироком від 7 серпня 2006 р. призначив А. кримінальне покарання, в тому числі й за ч. 1 ст. 3611 КК. З матеріалів справи вбачається, що А. з метою безкоштовного доступу до мережі Інтернет створив та використав шкідливу комп’ютерну програму, призначену для сканування мережі провайдера й отримання логінів та паролів, для модемного доступу до мережі Інтернет, які містилися на сервері провайдера. В подальшому А. незаконно використовував логіни та паролі для доступу до мережі Інтернет.

Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в ЕОМ, АС, комп’ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до вимог чинного законодавства, утворюють склад злочину, передбачений ст. 3612 КК. Ознакою комп’ютерної інформації з обмеженим доступом є те, що вона повинна бути створена та захищена відповідно до положень чинного законодавства, зокрема положень відповідних законів чи підзаконних нормативно-правових актів, у яких регламентується порядок її створення і захисту.

Комп’ютерна інформація з обмеженим доступом може бути конфіденційною і таємною, зокрема такою, що містить банківську чи комерційну таємницю.

Наприклад, Індустріальний районний суд м. Дніпропетровська вироком від 26 червня 2006 р. визнав Д. винним за ч. 1 ст. 3612 КК і призначив йому відповідне покарання. З матеріалів справи вбачається, що Д. відповідно до своїх службових повноважень мав доступ до комп’ютерної інформації про наступну переоцінку товарів у мережі магазинів, що було комерційною таємницею підприємства, в якому він працював. Цю інформацію він через мережу Інтернет розповсюдив серед осіб, які не були співробітниками цього підприємства і не мали права доступу до неї.

У ст. 362 КК передбачено відповідальність за несанкціоновані дії з інформацією, яка оброблюється в ЕОМ, АС, комп’ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

Об’єктивна сторона такого злочину полягає у вчиненні щодо відповідної комп’ютерної інформації несанкціонованих: 1) зміни; 2) знищення; 3) блокування; 4) перехоплення; 5) копіювання. У двох останніх випадках обов’язковим елементом об’єктивної сторони злочину є наслідки у вигляді витоку інформації.

Суб’єктом цього злочину може бути особа, яка має право доступу (на підставі трудових чи договірних правовідносин або з інших юридичних підстав) до комп’ютерної інформації чи носіїв такої інформації [8].

Суди при розгляді справ цієї категорії допускають помилки при кваліфікації дій винних осіб, які, маючи право доступу до комп’ютерної інформації, вчинювали щодо неї несанкціоновані дії.

Так, Заводський районний суд м. Миколаєва вироком від 14 березня 2007 р. визнав С. винним за ч. 1 ст. 3611 та ч. 2 ст. 15, ч. 1 ст. 361 КК і призначив йому відповідне покарання. З матеріалів справи вбачається, що С., працюючи інженером супроводження програмного забезпечення відділення ЗАТ КБ «ПриватБанк», відповідно до своїх службових обов’язків через локальну мережу мав доступ до всіх ЕОМ відділення банку. С. був незадоволеним розміром заробітної плати, з помсти за це керівництву банку, використовуючи наданий йому комп’ютер, за допомогою локальної комп’ютерної мережі зайшов на сервер банку і з метою використання створив у ньому шкідливий програмний засіб. Маючи намір запустити його та знищити інформацію, що містилася в ЕОМ відділення банку, напередодні свого звільнення розмістив його в активному стані у каталогах операційної системи серверу банку. Але реалізувати до кінця свій умисел, спрямований на несанкціоноване втручання в роботу сервера, яке могло призвести до втрати інформації, не зміг, оскільки в день подання заяви про звільнення йому було відмовлено в допуску до робочого місця і сервера.

Районний суд, кваліфікуючи дії С. за ч. 2 ст. 15, ч. 1 ст. 361 КК, припустився помилки, оскільки С. як відповідальна за експлуатацію АС особа намагався умисно знищити інформацію, яка в них оброблялася. У цьому випадку його дії слід було кваліфікувати за ч. 2 ст. 15, ч. 1 ст. 362 КК.

За несанкціоноване перехоплення або копіювання інформації, яка оброблюється в ЕОМ, АС, комп’ютерних мережах або зберігається на носіях такої інформації, вчинене особою, яка має право доступу до такої інформації, якщо ці дії призвели до її витоку, настає відповідальність, передбачена ч. 2 ст. 362 КК.

Наприклад, Жовтневий районний суд м. Дніпропетровська вироком від 27 липня 2007 р. визнав С. винною за ч. 2 ст. 362 КК та призначив їй відповідне покарання. С., працюючи у відділенні ЗАТ КБ «ПриватБанк» спеціалістом відділу кредитування фізичних осіб і маючи доступ до бази даних клієнтів та їхніх рахунків, скопіювала інформацію, що стосувалася рахунку одного з клієнтів банку (трансфер та комп’ютерні паролі входу до рахунку). Використовуючи зазначену інформацію, С. через мережу Інтернет поповнювала рахунок свого мобільного телефону та сплачувала рахунки за комунальні послуги.

У випадках зміни, знищення, блокування інформації злочин вважається закінченим з моменту фактичної зміни, знищення чи блокування відповідної інформації, а в разі перехоплення чи копіювання інформації — з моменту настання наслідків, спеціально передбачених законом.

Проте деякі суди при відмежуванні закінченого складу цього злочину від замаху на його вчинення допускали помилки.

Наприклад, вироком Ленінського районного суду м. Миколаєва від 29 травня 2006 р. за ч. 2 ст. 15, ч. 2 ст. 362 КК засуджено П., який, працюючи спеціалістом технічної підтримки канадської компанії та маючи доступ до інформації, яка оброблялась і зберігалася в комп’ютерній мережі компанії, вчинив несанкціоноване копіювання трьох шаблонів сайтів, які продав за 30 доларів США, що призвело до витоку цієї інформації. В цьому випадку суд помилково кваліфікував дії П. як замах на вчинення злочину, передбаченого ч. 2 ст. 362 КК, хоча в результаті його дій зазначена інформація стала відомою та доступною стороннім особам, тобто наявний закінчений склад злочину.

Крім того, дії П. слід було додатково кваліфікувати за ч. 1 ст. 3612 КК, оскільки він також здійснив несанкціонований збут інформації з обмеженим доступом.

Кримінальна відповідальність за порушення правил експлуатації ЕОМ, АС, комп’ютерних мереж чи мереж електрозв’язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК), настає, якщо цими діями заподіяно значну шкоду особою, яка відповідає за їх експлуатацію, за умови, що це спричинило викрадення, перекручення чи знищення комп’ютерної інформації, засобів їх захисту, або незаконне копіювання комп’ютерної інформації, чи істотне порушення роботи таких машин, їх систем чи комп’ютерних мереж [8].

Правилами експлуатації ЕОМ, АС, комп’ютерних мереж чи мереж електрозв’язку слід розуміти будь-які технічні правила, що регламентують порядок використання таких машин і автоматичної обробки в них інформації, а також забезпечення засобів захисту їх програмного забезпечення. У вироку суд має вказати, які конкретно правила були порушені винною особою. Саме ж порушення правил може бути як умисним, так і необережним. Між діями, що утворюють об’єктивну сторону цього злочину, і суспільно небезпечними наслідками має бути причинний зв’язок.

Порушення правил експлуатації ЕОМ, АС чи комп’ютерних мереж визнаються злочином лише в разі, коли їх наслідком було заподіяння значної шкоди, розмір якої визначено у примітці до ст. 361 КК. При цьому шкода, що береться до уваги при кваліфікації злочину, може стати значною як результат одного із допущених порушень або як сукупний результат усіх допущених порушень.

Суб’єкт зазначеного злочину спеціальний — особа, яка відповідає за експлуатацію ЕОМ, АС та комп’ютерних мереж.

Порушення правил експлуатації може виявлятися як в активних діях, коли особа вчинює дії всупереч розпорядженням, закріпленим у правилах, так і у формі бездіяльності — це невиконання або неналежне виконання обов’язків із технічного забезпечення захисту комп’ютерної інформації.

У ст. 3631 КК передбачено відповідальність за умисне масове розповсюдження повідомлень електрозв’язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи ЕОМ, АС, комп’ютерних мереж чи мереж електрозв’язку. Засобом вчинення такого злочину є повідомлення електрозв’язку, які розповсюджуються через систему ЕОМ, АС, комп’ютерні мережі чи мережі електрозв’язку, в тому числі через мережу Інтернет. Суспільно небезпечними наслідками злочину, склад якого передбачено ст. 3631 КК, є порушення або припинення роботи ЕОМ, АС, комп’ютерних мереж чи мереж електрозв’язку.

Розвиток мережі Інтернет призвів до того, що однією з основних проблем користувачів став надлишок інформації. Це стосується передусім так званого «спаму», тобто масового розповсюдження попередньо не обумовлених електронних листів. Через масовий характер спамових повідомлень останні утруднюють роботу інформаційних систем і ресурсів, створюючи для них зайве перевантаження, що може бути причиною їх виходу з ладу. «Спам» також може стати носієм шкідливих програм і комп’ютерних вірусів, поширених із метою отримання доступу до комп’ютерних систем, виведення їх із ладу або отримання конфіденційної інформації.

Однією з характерних особливостей цього виду злочинів є їхня латентність, яка спричинена небажанням користувачів мережі інформувати про такі злочини через недовіру до потенційних можливостей правоохоронних органів, а також небажанням публічно визнати слабкі місця у власних системах безпеки.

Згідно зі статистичною інформацією ДСА, у 2007-2009 рр. суди не розглядали кримінальних справ про злочини, передбачені статтями 363 та 3631 КК.

Вивчення зазначеної категорії кримінальних справ засвідчило, що суди, призначаючи покарання, здебільшого дотримуються передбаченого законом принципу індивідуалізації покарання залежно від характеру і ступеня тяжкості вчиненого злочину. Однак при призначенні покарань ще мають місце недоліки, на які необхідно звернути увагу. Зокрема, у деяких випадках сумнівними є рішення суду щодо призначення більш м’якого покарання, ніж передбачено законом, та звільнення осіб від відбування покарання з випробуванням. Згідно з вимогами ст. 69 КК суд може призначити більш м’яке покарання, ніж передбачено законом, лише за наявності декількох обставин (тобто не менше двох), що пом’якшують покарання та істотно знижують ступінь тяжкості вчиненого злочину, з урахуванням особи винного.

Однак мали місце випадки необґрунтованого призначення судами більш м’якого покарання, ніж передбачено законом [8].

Наприклад, Павлоградський міськрайонний суд Дніпропетровської області вироком від 30 квітня 2007 р. визнав П. винною за ч. 3 ст. 362 КК та із застосуванням ст. 69 цього Кодексу призначив їй покарання у виді двох років обмеження волі. Призначаючи П. покарання, суд у вироку зазначив лише про наявність позитивної характеристики підсудної, а обставин, які пом’якшують покарання, не навів.

У деяких випадках суди при призначенні покарання не враховують, що від конфіскації майна як виду додаткового покарання необхідно відрізняти спеціальну конфіскацію, яка полягає у вилученні у засудженого програмних або технічних засобів, за допомогою яких було вчинено злочин. Оскільки законом не передбачено можливості звільнення від такої конфіскації, спеціальна конфіскація має застосовуватися судами незалежно від застосування статей 69, 75 КК.

Так, Шевченківський районний суд м. Києва вироком від 10 березня 2006 р. визнав Я. винним у вчиненні злочину, передбаченого ч. 1 ст. 361 КК, та призначив йому покарання у виді трьох років обмеження волі з конфіскацією телефонного шлюзу «Audio codes», який є власністю винної особи та за допомогою якого він вчинив несанкціоноване втручання у мережу електрозв’язку. На підставі ст. 75 КК суд звільнив його від відбування покарання з випробуванням, зазначивши у вироку про звільнення його від конфіскації технічного засобу, за допомогою якого було вчинено несанкціоноване втручання.

Апеляційний суд м. Києва вирок районного суду скасував у частині призначення Я. покарання та постановив свій вирок, яким призначив йому відповідне покарання із застосуванням конфіскації телефонного шлюзу.

Проведене узагальнення засвідчило, що при розгляді зазначеної категорії справ суди допускають помилки при кваліфікації дій винних осіб, розрізненні одних злочинів від інших, вирішенні питань про наявність або відсутність кваліфікуючих ознак та призначенні кримінального покарання.

Труднощі також виникають при кваліфікації дій винних осіб, коли несанкціоноване втручання в роботу ЕОМ, АС, комп’ютерних мереж здійснювалося з корисливих мотивів із метою викрадення чи заволодіння чужим майном. Зазначені дії суди помилково кваліфікують лише за статтями КК, в яких передбачено відповідальність за вчинення комп’ютерних злочинів [8].

Призначаючи покарання за вчинення такого виду злочинів, суди іноді не застосовують обов’язкову конфіскацію програмних та технічних засобів, за допомогою яких було вчинено злочин.

**ЗАДАЧІ**

**Задача 1**

**Шемаченко у відсутність чоловіка, що знаходився у тривалому відрядженні, підгримувала статеві зв'язки з Коваленко. Через певний час вона завагітніла і, побоюючись розправи з боку чоловіка, вирішила позбавитися дитини. Про свій намір вона повідомила знайому Кириченка, яка згодилася за певну винагороду їй допомогти. Коли дитина народилася, то Кириченко прийняла пологи, а наступного дня вони втопили дитину у ванні, а труп закопали.**

**Кваліфікуйте дії вказаних осіб.**

Дії Шемаченко слід кваліфікувати за ст. 117 КК України як умисне вбивство матір'ю своєї новонародженої дитини. Якщо умисне вбивство матір'ю своєї новонародженої дитини вчинено із заздалегідь обдуманим умислом, у т.ч. за взаємною згодою подружжя, вчинене слід кваліфікувати за п. 2 ч. 2 ст. 115, а за наявності підстав - і за іншим пунктом ч. 2 цієї статті.

Об'єктом злочину є життя новонародженої особи.

Потерпілим від цього злочину може бути лише власна новонароджена дитина матері.

Об'єктивна сторона злочину характеризується; 1) діями - посяганням на життя іншої новонародженої дитини; 2) наслідками у вигляді її смерті; 3) причинним зв'язком між зазначеними діями та наслідком, а також 4) часом і певною обстановкою - це діяння може бути вчинено лише під час пологів або відразу після пологів.

Суб'єктом злочину може бути лише мати потерпілої дитини, яка є осудною і на момент вчинення злочину досягла 14-річного віку.

Умисне вбивство матір'ю своєї новонародженої дитини у даній ситуації вчинене у співучасті. Співвиконавець цього вбивства (Кириченко) підлягає кримінальній відповідальності залежно від обставин справи за відповідною частиною (і пунктом ч. 2) ст. 115. Дії підбурювача і пособника кваліфікуються відповідно, за ч. ч. 3 або 4 ст. 27 і ст. 117.

Суб'єктивна сторона характеризується прямим або непрямим умислом. Психічне ставлення особи при вчиненні цього злочину характеризують такі особливості: 1) його вчинення обумовлене емоційною напругою, викликаною вагітністю і пологами та психічними процесами, що їх супроводжували (зокрема сімейним конфліктом, подружньою зрадою, матеріальними та іншими соціально-побутовими негараздами); 2) тимчасовий психічний розлад послаблює здатність матері усвідомлювати свої дії та керувати ними, у зв'язку з чим вона є обмежено осудною.

**Задача 2**

**Колишній слідчій Кругових, який вже рік не працював, вийшовши на пенсію, на стадіоні під час футбольного матчу зустрівся з Дмитренком, якого він раніше притягав до кримінальної відповідальності. Зі словами: "Тепер будеш знати як сажати невинних у тюрму!" - Дмитренко наніс удар ножем у живіт Кругових. Через декілька хвилин потерпілого доставили до лікарні, де вдалося врятувати йому життя.**

**Кваліфікуйте дії Дмитренка.**

Так як Круговий колишній слідчий, то дії Дмитренка слід кваліфікувати за ч. 3 ст.345 КК України як умисне заподіяння працівникові правоохоронного органу або його близьким родичам тяжкого тілесного ушкодження у зв'язку з виконанням цим працівником службових обов'язків.

Основним безпосереднім об'єктом злочину є нормальна діяльність правоохоронних органів, їх авторитет, а додатковим обов'язковим об'єктом - психічна недоторканність працівників правоохоронних органів або їх близьких родичів, їх здоров'я.

Потерпілими від цього злочину можуть бути: 1) працівник правоохоронного органу, 2) його близькі родичі.

Об'єктивна сторона злочину може бути виражена у: 1) погрозі (ч 1 ст 345); 2) заподіянні побоїв, а також тілесних ушкоджень - легких, середньої тяжкості (ч. 2 ст. 345) або тяжких (ч. 3 ст. 345).

Злочин вважається закінченим з моменту висловлення погрози (ч. 1 ст. 345), заподіяння побоїв чи тілесних ушкоджень (ч. 2 ст. 345).

Суб'єктом цього злочину у вигляді погрози, заподіяння побоїв або легких тілесних ушкоджень може бути осудна особа, яка досягла 16-річного віку, а у вигляді заподіяння середньої тяжкості або тяжких тілесних ушкоджень - 14-річного віку.

Суб'єктивна сторона злочину характеризується прямим умислом.

**ВИСНОВКИ**

Розвиток методів обробки інформації за допомогою комп'ютерів призвів до застосування цих машин в усіх галузях національної економіки та інших сферах суспільного життя. Значна кількість таких машин об'єднана комп'ютерними мережами, деякі з них набули інтернаціонального характеру. За цих умов виникли і набули суспільної небезпеки різні діяння, що заподіюють шкоду нормальній роботі комп'ютерів та комп'ютерних мереж, яка поряд зі встановленим порядком використання ЕОМ та комп'ютерних мереж становить об'єкт цього злочину.

Предметом злочину є: 1) автоматизовані електронно-обчислювальні машини (комп'ютери, АЕОМ), у т.ч. персональні; 2) їх системи; 3) комп'ютерні мережі.

Об'єктивна сторона злочину проявляється у формі: 1) незаконного втручання у роботу АЕОМ, їх систем чи комп'ютерних мереж, що призвело до перекручення чи знищення комп'ютерної інформації або носіїв такої інформації; 2) розповсюдження комп'ютерного вірусу. Суб'єкт злочину загальний.

Суб'єктивна сторона злочину характеризується умисною виною, Злочинні дії можуть бути вчинені лише з прямим умислом, тоді як ставлення винного до наслідків злочину може характеризуватись як прямим, так і непрямим умислом. Кваліфікуючими ознаками (ч. 2 ст. 361) злочину є вчинення його: 1) повторно; 2) за попередньою змовою групою осіб; 3) заподіяння ним істотної шкоди. Слід наголосити на практичній доцільності виокремлення і розгляду як самостійних юридичних складів злочинів “Несанкціонований доступ до комп’ютерної інформації” та “Умисне розповсюдження шкідливих комп’ютерних програм”, альтернативних діянь, передбачених чинною редакцією ч.1 ст. 361 КК України. Слід закріпити вказані юридичні склади в окремих статтях Особливої частини КК України.

**СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ**

1. Конституція України від 28 червня 1996 р. // Відомості Верховної Ради України. — 1996. — № 30. — Ст. 141.
2. Кримінальний кодекс України від 5 квітня 2001 року.
3. Закон України «Про інформацію» від 2 жовтня 1992 р. № 2657-ХІІ
4. Закон України «Про науково-технічну інформацію» вiд 25 червня 1993 р. № 3322-XII
5. Закон України «Про телекомунікації» від 18 листопада 2003 р. № 1280-ІV
6. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 р. № 80/94-ВР.
7. Положення про технічний захист інформації в Україні (затверджене Указом Президента України від 27 вересня 1999 р. № 1229/99).
8. Узагальнення судової практики Верховного Суду України „Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), автоматизованих систем та комп’ютерних мереж і мереж електрозв’язку” від 19.10.2009 року.
9. Александров Ю.В., Антипов В.І., Дудоров О.О. та ін. Кримінальне право України: загальна та особлива частини. Підручник у 2-х тт. / За ред. Мельника М.І., Клименка В.А. - К.: Юридична думка, 2004. - 352/656 с.
10. Андрушко П.П., Кобзаренко В.П., Матишевский П.С., Шапченко С.Д. Кримінальне право України: практикум / За ред. Яценко С.С. - К.: Юрінком Інтер, 2004. – 592 с.
11. Вовкотруб С.Г., Омельчук О.М., Ярін В.М. та ін. Кримінальне право України / За ред. Омельчука О.М. - К.: Наукова думка, 2004. – 297 с.
12. Голубєв В.О., Гавловський В.Д., Цимбалюк В.С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп’ютерних технологій. / За заг. ред. д.ю.н., професора Калюжного Р.А. - Запоріжжя: Просвіта, 2001. - 257с.
13. Кримінальний кодекс України: Наук.-практ. коментар / За заг. ред. В.В. Сташиса, В.Я. Тація. — К., 2006. — С. 969.
14. Кузнецов В.В., Савченко А.В. Кримінальне право України. - К.: Паливода, 2006. – 300 с.
15. Кузнєцов В.О., Стрельбицький М.П., Гіжевський В.К. Кримінальне право України: Загальна та Особлива частини. - К.: Істина, 2005. – 380 с.
16. Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001 року / За ред. М.І. Мельника, М.І. Хавронюка. — К.: Каннон, А.С.К., 2003. – 1230 с.
17. Пашнєв Д.В., Рудик М.В. Особливості виявлення та кримінально-правова кваліфікація злочинів, що посягають на комп’ютерну інформацію з обмеженим доступом // Ученые записки Таврического национального университета им. В. И. Вернадского / Серия «Юридические науки». - Том 22 (61). - № 1. - 2009. - С. 229-235.
18. Розенфельд Н.А. Відповідальність за незаконне втручання в роботу ЕОМ (комп’ютерів)// Вісник прокуратури. - 2002. - № 4. - С. 23-27.
19. Розенфельд Н.А. Деякі аспекти вдосконалення відповідальності за незаконне втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж// Матеріали науково-практичної конференції “Становлення і розвиток правової системи України”: Тези доповідей і наук. повідомлень. - К.: НАН України, Інститут держави і права ім. В.М.Корецького. - 2002. - С. 186-188.
20. Розенфельд Н.А. Деякі особливості визначення ознак об’єктивної сторони складу злочину “Незаконне втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж”// Адвокат. - 2002. - № 4-5. - С. 24-26.
21. Розенфельд Н.А. Загальна характеристика умисних комп’ютерних злочинів// Право України. - 2002. - № 9. - С. 88-93.
22. Розенфельд Н.А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж. - Рукопис. Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.08. - кримінальне право та кримінологія; кримінально-виконавче право. - Інститут держави і права ім. В.М.Корецького НАН України, Київ, 2003. – 230 с.
23. Розенфельд Н.А. Проблеми вдосконалення відповідальності за незаконне втручання в роботу електронно-обчислювальних машин (комп’ютерів), їх систем та комп’ютерних мереж// Держава і право: Збірник наукових праць. Юридичні і політичні науки. - К.: Ін-т держави і права ім. В.М.Корецького НАН України; Спілка юристів України. - 2002. - Вип. 16. - С. 355-359.
24. Розенфельд Н.А. Програмно-математичні заходи захисту комп’ютерної інформації як предмет злочину “Незаконне втручання в роботу ЕОМ (комп’ютерів), систем та комп’ютерних мереж” // Збірник наукових праць за матер. наук. конф. студентів і аспірантів “Актуальні проблеми правознавства очима молодих вчених”. - Хмельницький: Хмельницький інститут управління і права. - 2002. - С. 229-230.
25. Розенфельд Н.А. Спосіб та знаряддя вчинення злочину “Незаконне втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж”// Вісник Академії праці і соціальних відносин Федерації профспілок України: матеріали міжнар. наук. конф. “Україна: шляхами віків”, присвяченої 175-річчю з дня народження Георгія Андрузького: У 2-х ч. - К.: Академія праці і соціальних відносин Федерації профспілок України. - 2002. - Ч. 1. - С. 204-207.
26. Савченко А.В., Кузнецов В.В., Штанько О.Ф. Сучасне кримінальне право України. - К.: Паливода, 2006. – 636 с.
27. Стратонов В.М., Сотула О.С. Кримінальне право України: Загальна та Особлива частини. - К.: Істина, 2007. – 400 с.