МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ЛУГАНСЬКА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
ІМЕНІ 10-РІЧЧЯ НЕЗАЛЕЖНОСТІ УКРАЇНИ

На правах рукопису

КАРЧЕВСЬКИЙ МИКОЛА ВІТАЛІЙОВИЧ

УДК 343.346.8

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА НЕЗАКОННЕ ВТРУЧАННЯ В РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ

(аналіз складу злочину)

Спеціальність 12.00.08. – кримінальне право та кримінологія;
кримінально-виконавче право

Дисертація на здобуття наукового ступеня
кандидата юридичних наук

Науковий керівник:
Кривоченко Людмила Миколаївна
кандидат юридичних наук професор

ЛУГАНСЬК – 2003

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Право - регулятор суспільних відносин. Тому зміни в структурі та змісті суспільних відносин повинні знаходити відображення в нормах права. Зокрема, істотні зміни в суспільних відносинах на сучасному етапі розвитку викликані науково-технічним прогресом. Впровадження новітніх технологій в усі сфери життя суспільства неминуче призводить до значного розширення інформаційних потоків ("інформаційний вибух"), зростання інформаційної потреби. Щоб діяти ефективно, сучасній людині необхідно мати набагато більший обсяг інформації, ніж людині, яка жила, наприклад, на початку XX століття.

З процесом інформатизації тісно пов'язаний процес комп'ютеризації: розвиток і впровадження в різні сфери життя та діяльності людини технічної бази, яка забезпечує оперативне одержання результатів опрацювання інформації та її накопичення.

Розширення сфери застосування комп'ютерних технологій, без сумніву, має позитивне значення для розвитку суспільних відносин у сфері інформатизації. Однак воно спричиняє і негативні наслідки: появу нового виду злочинів - злочинів у сфері використання електронно-обчислювальних машин, систем і комп'ютерних мереж. Це ставить перед державою та суспільством завдання щодо розроблення засобів і методів боротьби з зазначеними злочинами, створення нормативної бази для його вирішення.

Новий Кримінальний кодекс України вперше передбачив самостійний розділ про ці злочини - розділ XVI "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж", який і є такою нормативною базою. У зв'язку з цим актуальним є науковий аналіз злочинів, передбачених статтями даного розділу, і зокрема статтею 361 "Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж".

До цього часу не було самостійної наукової роботи, яка б спеціально присвячувалася характеристиці цього злочину. Окремі аспекти кримінальної відповідальності за незаконне втручання досліджувалися такими вченими, як Ю.М. Батурін, П.Д. Біленчук, А.Б. Венгеров, В.В. Вертузаєв, М.В. Вєхов, О.Г. Волєводз, О.А. Гаврилов, В.В. Голіна, В.В. Голубєв, П.А. Дубров, А.М. Жодзишський, М.А. Зубань, Р.А. Калюжний, М.М. Коваленко, В.В. Кузнєцов, Ю. Ляпунов, В. Максимов, М.І. Панов, В.В. Пивоваров, М.С. Полєвой, В.А. Северин, С.І. Семилєтов, К.С. Скоромніков, Ф.П. Тарасенко, Л.К. Терещенко, Б.С. Українцев, В.С. Фролов, А.В. Черних.

Викладені положення і зумовили вибір теми дисертації, у якій здійснено спробу дослідити кримінально-правовий зміст об'єктивних і суб'єктивних ознак складу злочину, передбаченого статтею 361 КК, проаналізувати його співвідношення з іншими злочинами цього розділу, а також відмежувати його від інших злочинів, пов'язаних з використанням ЕОМ.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано згідно з планами науково-дослідної роботи Луганської академії внутрішніх справ МВС імені 10-річчя незалежності України. Тема дисертації відповідає пріоритетним напрямкам наукових досліджень вищих навчальних закладів системи МВС, визначеним Наказом МВС України № 356 від 11 травня 2001 року "Про затвердження Програми розвитку відомчої освіти та вузівської науки на період 2001-2005 років" (п. 7).

Мета і задачі дослідження. Мета полягає в юридичному аналізі складу незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (у подальшому викладенні матеріалу назва злочину, що аналізується, буде скорочена – "незаконне втручання"), формулюванні можливих змін і доповнень до чинного законодавства. Для досягнення цієї мети було поставлено такі завдання:

- визначити родовий і безпосередній об'єкти незаконного втручання;

- встановити ознаки предмета цього злочину;
- розкрити зміст поняття "незаконне втручання";
- показати специфіку суб’єктивної сторони цього злочину;
- визначити критерії відмежування незаконного втручання від суміжних злочинів;
- сформулювати пропозиції щодо внесення змін і доповнень до чинного КК України.

Об’єктом дослідження виступає незаконне втручання в роботу електронно-обчислювальних машин як один із видів злочинів у сфері використання електронно-обчислювальних машин, систем та комп’ютерних мереж, а також соціальна зумовленість кримінальної відповідальності за цей злочин, його специфічні об’єктивні та суб’єктивні ознаки.

Предметом дослідження є норми чинного кримінального законодавства, практика їх застосування, тенденція та закономірності розвитку кримінального законодавства про відповідальність за незаконне втручання в роботу електронно-обчислювальних машин, систем та комп’ютерних мереж, його наукове тлумачення.

Методи дослідження. Методологічною основою є комплексний підхід до аналізу незаконного втручання. Для дослідження застосовувалися такі наукові методи:

- логіко-історичний, який дозволив проаналізувати розвиток об’єкта дослідження;
- системного аналізу соціальних явищ, за допомогою якого досліджувався зміст інформаційних відносин;
- догматичний – для дослідження змісту законодавчих положень про незаконне втручання;
- порівняльно-правовий, що дав можливість порівняти вітчизняне законодавство про незаконне втручання з відповідними

положеннями кримінального законодавства зарубіжних країн, тощо.

У процесі написання використовувалися досягнення кримінального, цивільного права, загальної теорії права, інформатики та ін.

Наукова новизна одержаних результатів полягає в тому, що дисертація є першим в Україні дисертаційним дослідженням проблем кримінальної відповідальності за незаконне втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж за новим Кримінальним кодексом України. Новими, на погляд автора, є такі положення.

1. Вперше розкривається кримінально-правовий зміст інформаційних відносин у сфері використання комп'ютерної техніки як родового об'єкта злочинів, передбачених розділом XVI КК України, і обґрунтовується пропозиція про доцільність визначення їх загальним терміном "комп'ютерні злочини"

2. На підставі визначення родового об'єкту вперше розкривається зміст безпосереднього об'єкта незаконного втручання як суспільних відносин власності на комп'ютерну інформацію. Відповідно, по-новому визначається комп'ютерна інформація як предмет цього злочину і вносяться пропозиції про недоцільність передбачення в диспозиції ст. 361 КК України вказівки на носії інформації як самостійний предмет незаконного втручання.

3. Визнано необґрунтованим передбачення комп'ютерного вірусу в ч. 1 ст. 361 КК України як самостійного предмету злочину. Замість цього пропонується визначити предметами незаконного втручання програмні і технічні засоби, призначені для незаконного, втручання до яких відносяться і комп'ютерні віруси.

4. По-новому визначаються знищення та перекручення комп'ютерної інформації як різні форми порушення права власності на комп'ютерну інформацію.

5. Вперше у вітчизняній науці здійснено спробу класифікації способів незаконного втручання, що має важливе значення для встановлення об'єктивної сторони та ступеня суспільної небезпечності злочину, що досліджується.

6. Вперше доводиться необхідність доповнення ч. 2 ст. 361 КК України такими кваліфікуючими ознаками, як "вчинення незаконного втручання шляхом несанкціонованого доступу до комп'ютерної інформації" і "вчинення незаконного втручання особою, яка має доступ до роботи на ЕОМ, у системі чи комп'ютерній мережі у зв'язку з виконуваною роботою або займаною посадою".

7. Обґрунтовується вперше необхідність доповнення статті 361 КК України частиною 3, яка б передбачала відповідальність за незаконне втручання, що спричинило тяжкі наслідки, та розкривається зміст таких наслідків.

8. Пропонується нова редакція статті 361 КК України "Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж".

Практичне значення одержаних результатів зумовлюється таким:

- у науково-дослідній роботі висновки й положення дисертаційного дослідження можуть бути використані в процесі подальшого розроблення проблем кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин, систем і комп'ютерних мереж;

- для правотворчої діяльності пропонується модель кримінально-правової норми про відповідальність за незаконне втручання в роботу електронно-обчислювальних машин шляхом несанкціонованого доступу до комп'ютерної інформації, яка може бути використана з метою подальшого вдосконалення кримінального законодавства;

- у правозастосовчій діяльності запропоновані висновки можуть бути використані при кваліфікації злочинів у сфері використання електронно-обчислювальних машин, їх систем і комп'ютерних мереж;

- у навчальному процесі матеріали дисертаційного дослідження можуть бути використані в процесі викладання курсу Особливої частини кримінального права України, при підготуванні навчальної та методичної літератури з відповідної тематики, при проведенні науково-дослідної роботи студентів (курсантів).

Апробація результатів дисертації. Дисертацію обговорено на засіданні кафедри кримінального права та кримінології Луганської академії внутрішніх справ МВС імені 10-річчя незалежності України. Результати досліджень, котрі містяться в дисертації, викладені на міжнародній науково-практичній конференції "Проблеми вдосконалення законодавства з урахуванням прогнозу злочинності" (Луганськ, 1999 р.), міжвузівській науково-практичній конференції "Правові основи захисту комп'ютерної інформації від протиправних посягань" (Донецьк, 2000 р.) і міжнародній науково-практичній конференції "Нове кримінальне і кримінально-процесуальне законодавство та завдання юридичної підготовки кадрів ОВС України" (Луганськ, 2002 р.).

Публікації. За темою дисертації автором опубліковано монографію, п'ять наукових статей у спеціалізованих наукових виданнях, перелік яких затверджено ВАК України, тези трьох наукових доповідей.

Структура дисертації. Відповідно до мети та завдань дослідження, його предмета і логіки дисертація складається із вступу, п'яти розділів, висновків та списку використаних джерел. Повний обсяг дисертації – 175, із них список використаних джерел – 16 сторінок (166 найменувань).

Розділ 1
ОБ'ЄКТ І ПРЕДМЕТ НЕЗАКОННОГО ВТРУЧАННЯ В РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН, СИСТЕМ І КОМП'ЮТЕРНИХ МЕРЕЖ

1.1. Проблема об'єкта злочину в науці кримінального права

Проблема об'єкта злочину – одна з найважливіших у науці кримінального права. Будь-яке кримінально-правове дослідження проблеми відповідальності за конкретний злочин насамперед як вихідну позицію передбачає аналіз об'єкта злочину. І це цілком обґрунтовано тим значенням, яке має об'єкт для визначення соціальної сутності злочину, ступеню його тяжкості, місця в системі злочинів, для правильної його кваліфікації та відмежування від суміжних складів. Врешті-решт, сама кримінально-правова заборона зумовлена заподіянням шкоди об'єкту і саме об'єкт зумовлює межі цієї заборони.

Оцінюючи значення об'єкта, Н.Ф. Кузнєцова правильно підкреслює, що "без об'єкта посягання немає і злочину".[1] Ось чому аналіз об'єкта справедливо можна визнати методологічною основою кримінально-правових досліджень усіх конкретних складів злочинів. Не втратило своєї актуальності сказане ще Б.С. Утевським: "За об'єктом злочину приховується перш за все природа тієї чи іншої категорії злочинів, того чи іншого конкретного складу".[2] Об'єкт злочину визначає механізм самого впливу на нього, а отже, визначає і специфіку ознак об'єктивної сторони злочину, характеризуючи діяння, спосіб його здійснення, характер шкоди тощо. Не менш важливим є значення

---

[1] [83] Курс уголовного права. Общая часть. Том 1: Учение о преступлении: Учебник для вузов /Под ред. Н.Ф. Кузнецовой, И.М. Тяжковой. – М.: Зерцало, 1999. – С. 198.

[2] [146] Утевский Б.С. Общее учение о должностных преступлениях. – М.: Юридическое издательство, 1948. – С. 292.

об’єкта і для встановлення суб’єктивної сторони: форми і виду вини, мотивів і мети скоєння злочину.

Протягом багатьох років у науці кримінального права України, Росії та інших країн СНД було загальновизнаним, що об’єкт злочину – це суспільні відносини, на які посягає злочин, завдаючи їм певної шкоди, і які знаходяться під охороною закону про кримінальну відповідальність.[1] Ще в 1924 році А.А. Піонтковський писав, що суспільні відносини є загальним об’єктом, на який, врешті-решт, посягає будь-який злочин, передбачений кримінальним законом.[2] Однак останніми роками ця позиція піддається перегляду. З’явилася думка, що таке розуміння об’єкта є застарілим і не дозволяє правильно визначити об’єкт більшості злочинів. Так, А.В. Наумов, не заперечуючи, що в багатьох злочинах суспільні відносини – це об’єкт, стверджує, що на деякі злочини таке розуміння об’єкта не поширюється, і тому, на його думку, для встановлення об’єктів ряду злочинів необхідне "повернення до теорії об’єкта як правового блага, створеної ще наприкінці минулого століття в межах класичної та соціологічної шкіл кримінального права".[3]

Більш категорична А.В. Пашковська. Вона пропонує в усіх випадках вважати об’єктом злочину "охоронювані кримінальним законом соціально значущі цінності, інтереси, блага, на які посягає особа, котра скоїла злочин, і яким у результаті вчинення злочинного діяння заподіюється або може бути заподіяна шкода".[83][4]

---

[1] [71] Кримінальне право України: Загальна частина: Підручник для студентів юрид. спец. вищ. закладів освіти /М. І. Бажанов, Ю.В. Баулін, В.І. Борисов та ін.; За ред. професорів М.І. Бажанова, В.В. Сташиса, В.Я. Тація. – Київ-Харків: Юрінком Інтер-Право, 2001. – С. 90.
[2] [103] Пионтковский А.А. Учение о преступлении. – М.: Госюриздат, 1961. – С. 129-130.
[3] [94] Наумов А.В. Уголовное право. Общая часть: Курс лекций. – М.: БЕК, 1996. – С. 147.
[4] [83] Курс уголовного права. Общая часть. Том 1: Учение о преступлении: Учебник для вузов /Под ред. Н.Ф. Кузнецовой, И.М. Тяжковой. – М.: Зерцало, 1999. – С. 202.

В Україні розуміння об’єкта як цінностей відстоює Є.В. Фесенко.[1] На його думку, що об’єктом виступають, зокрема, "різноманітні об’єкти матеріального світу, у тому числі й сама людина, які мають істотне значення для окремих осіб, соціальних груп і суспільства в цілому".[2] До цінностей (об’єкта) він також відносить: потерпілого, інтереси і права, соціальний зв’язок, блага.

Не можна не сказати, що ця позиція не є новою. Ще М.С. Таганцев визнавав об’єктом правоохоронюваний інтерес життя, правове благо.[3] Цю позицію розвивав і Н.С. Бєлогриць-Котляревський, стверджуючи, що злочин, "порушуючи норми, тобто абстрактні заборони або веління закону, водночас необхідно руйнує ті реальні блага або інтереси, для яких ці блага існують. Порушуючи норму "не вкради", злодій водночас руйнує чиєсь майнове благо".[13][4]

Цікавої позиції дотримується Г.П. Новосьолов. Він вважає, що “об’єктом будь-якого злочину ... є люди, які в одних випадках виступають в якості окремих фізичних осіб, у других – як деякого роду множина осіб, які мають або не мають статус юридичної особи, у третіх – як соціум (суспільство)”.[5]

Для оцінки різних позицій щодо розуміння об’єкта не можна не враховувати, що блага, цінності, життєві інтереси тощо поза суспільними відносинами, які склалися у суспільстві на певному етапі його розвитку, не існують. Поняття "цінність", "благо", "інтерес" похідні від суспільства (тобто

---

[1] Див.: [147] Фесенко Є.В. Цінності як об’єкт злочину //Право України. – 1999. – № 6. – С. 75.; [70] Кримінальне право України. Загал. частина: Підручник для студентів вузів і факультетів /Г.В. Андрусів, П.П. Андрушко, В.В. Бенківський та ін.; За ред. П.С. Матишевського та ін. – К.: Юрінком Інтер, 1997. – С.123-132.

[2] [147] Фесенко Є.В. Цінності як об’єкт злочину //Право України. – 1999. – № 6. – С. 75.

[3] [129] Таганцев Н.С. Русское уголовное право. Лекции часть общая. В 2-х томах. Т. 1. – М., 1994. – С. 32-34.

[4] [13] Белогриц-Котляревский Н.С. Учебник русского уголовного права. Общая и особенная части. Украинское книгоиздательство. – Киев-Петербург-Харьков, 1903. – С. 161-162.

[5] [96] Новосёлов Г.П. Учение об объекте преступления. Методологические аспекты. – М.: Норма, 2001. – С. 60.

сукупності суспільних відносин), а тому і їх правова оцінка неможлива поза цими відносинами. Отже, правильним, на нашу думку, залишається розуміння об'єкта злочину як суспільного відношення. Таке розуміння підтверджується самим змістом будь-якого суспільного відношення, його структурою. Загальновизнано, що кожне суспільне відношення має складну структуру, складається з трьох взаємопов'язаних елементів:

1) носії (суб'єкти) відношення;
2) предмет, з приводу якого існує відношення;
3) соціальний взаємозв'язок.[1]

Якщо стати на позицію, що об'єкт – це інтереси, цінності, блага, то небезпечність злочину зводиться до завдання шкоди лише одному структурному елементу суспільного відношення. Не охороняються, залишаються незахищеними інші його елементи; не враховується, що в конкретному злочині шкода може завдаватися будь-якому з трьох елементів, що, однак, призводить до порушення всього суспільного відношення.

Необхідно також відзначити, що концепція цінностей як об'єкта злочину не дає дослідникові методологічної бази для аналізу механізму заподіяння шкоди, що надмірно ізолює об'єкт злочину від інших ознак складу, зменшує його системоутворююче значення. Тому вихідним положенням у дослідженні об'єкта незаконного втручання в роботу електронно-обчислювальних машин у даній роботі є розуміння його як суспільного відношення, яке охороняється кримінальним законом. Видається, що саме з такого розуміння виходить і КК України, формулюючи в ч. 1 ст. 1 завдання Кримінального кодексу: "Кримінальний кодекс України має своїм завданням правове забезпечення охорони прав і свобод людини, власності, громадського порядку і громадської безпеки, навколишнього природного середовища, конституційного устрою України від злочинних посягань,

[1] [132] Таций В.Я. Объект и предмет преступления в советском уголовном праве. – Х.: Вища шк.: Изд-во при ХГУ, 1988. – С. 16.

забезпечення миру і безпеки людства, а також попередження злочинів". У цій статті визначається загальний об’єкт, дається перелік усієї сукупності суспільних відносин, які охороняються законом про кримінальну відповідальність. Таке розуміння об’єкта рівною мірою відноситься до всіх його видів: загального, родового і безпосереднього.

Досліджуючи об’єкт злочину, передбаченого статтею 361, автор бере за основу загальновизнане положення про взаємовідношення цих видів: загальний об’єкт – це вся сукупність охоронюваних кримінальним законом відносин, родовий – певна група однорідних відносин, що охороняються групою норм КК, безпосередній – конкретне суспільне відношення, яке охороняється конкретною нормою КК. Таким чином, вони співвідносяться між собою як загальне – особливе – окреме.

1.2. Родовий об’єкт незаконного втручання в роботу ЕОМ

Достатньо обґрунтованим у науці кримінального права є положення про те, що неможливо дати глибокий аналіз безпосереднього об’єкта будь-якого злочину без встановлення тієї сфери (сукупності) суспільних відносин, які утворюють родовий об’єкт цього злочину. Це зумовлено тим, що саме родовий об’єкт виконує ряд важливих функцій:

1) характеризує суспільну небезпечність певних груп злочинів, які посягають на тотожні або однорідні суспільні відносини;

2) визначає місце конкретного злочину в системі Особливої частини КК, а, отже, дозволяє розмежувати подібні за об’єктивною та суб’єктивною стороною злочини, які посягають на різні родові об’єкти[1];

3) допомагає точніше визначити безпосередній об’єкт, який повинен бути частиною відносин, що утворюють родовий об’єкт.

[1] [152] Фролов Е.А. Спорные вопросы общего учения об объекте преступления: Сборник научных трудов. – Вып. 10. – Свердловск, 1969. – С. 184 - 225.

В Україні комп'ютерні технології впроваджено з істотним відставанням у часі й масштабах від передових західних країн, і дефіцит практики позначається на темпах формування законодавства. Так, за повідомленням Національного центрального бюро Інтерполу в Україні, куди згідно відомчих наказів надходить інформація про вчинення злочинів в сфері використання комп'ютерної техніки в Україні, у 2000 році "фактів, де комп'ютерна техніка виступала як об'єкт скоєння злочину, у тому числі фактів несанкціонованого проникнення до локальних відомчих комп'ютерних мереж та банків даних, зареєстровано не було".[1] Однак дана обставина створює також певні переваги в можливості використання західного досвіду правового регулювання. Причому, якщо безоглядне перенесення західних стандартів регулювання політичних, економічних і соціальних процесів без урахування історичних і національних особливостей України призвело до істотних недоліків, то техніка споконвічно безпартійна і поле для запозичення значно ширше. Тому аналіз законодавства зарубіжних країн з питань злочинів в сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж видається доречним, як приклад визначення родового об'єкту цих злочинів.

У країнах Західної Європи законодавець з питання злочинів у сфері використання комп'ютерних технологій пішов за двома напрямками:

– по-перше, багато статей про посягання на особу, власність і т.ін. були доповнені нормами про відповідальність за ці злочини у випадках їх скоєння з використанням комп'ютерної техніки;

– по-друге, до КК були внесені нові норми про відповідальність за посягання на якісно новий об'єкт, що й зумовило виникнення злочинів у

[1] [2] Аналітичний огляд стану комп'ютерної злочинності та інформаційної безпеки в Україні у 2000 році // Національне бюро Інтерполу в Україні. – К., 2001. – С. 6. (Наводиться за: [41] Гуцалюк М. Координація боротьби з комп'ютерною злочинністю // Право України. – 2002. – № 5. – С. 121.)

сфері використання електронно-обчислювальних машин, систем і комп'ютерних мереж.

Як приклад достатньо розглянути відображення цих двох напрямків у законодавстві ФРН і Франції. КК цих країн містять доповнення про вчинення посягань із використанням комп'ютерної техніки в нормах про злочини проти особи, власності, встановленого порядку обігу документів, проти національної безпеки, інтелектуальної власності, комерційної таємниці.

Так, наприклад, розділ 15 КК ФРН[1] – "Порушення недоторканності і таємниці приватного життя" – доповнено статтею 202а "Дії, спрямовані на одержання відомостей", у якій встановлюється відповідальність за незаконне одержання або передавання відомостей, "котрі можуть бути відтворені або передані електронним, магнітним або іншим способом і не є такими, що сприймаються безпосередньо". А до розділу 22 – "Шахрайство і злочинне зловживання довірою" – внесено статтю 263а "Комп'ютерне шахрайство", яка передбачає відповідальність за незаконне одержання вигоди або заподіяння шкоди майну іншої особи шляхом неправомірного впливу на процес опрацювання даних.

У КК Франції[1] Книга 2 "Про злочини і проступки проти людини" містить параграф 2 "Про посягання на таємницю кореспонденції", де в статті 226-15 встановлено відповідальність за порушення таємниці кореспонденції, яка передається за допомогою засобів комп'ютерної техніки. Книга 4 "Про злочини і проступки проти нації, держави та громадського порядку" містить статті 411-6 – 411-8, які передбачають відповідальність за передавання або забезпечення доступності для іноземної держави, іноземного підприємства чи організації або підприємства чи організації, котрі знаходяться під іноземним контролем, або їхнім представникам даних, що містяться в пам'яті ЕОМ, використання, розповсюдження або збирання яких може призвести до

[1] [143] Уголовный кодекс ФРГ /Пер. с нем. А.В. Серебренникова. – М., 1996.

посягання на основоположні інтереси нації; збирання та зосередження з метою передавання таких даних і здійснення за рахунок іноземних організацій діяльності, спрямованої на одержання зазначених даних.

Водночас, крім цих норм, у КК зазначених країн передбачені норми про відповідальність за посягання на відносини у сфері використання електронно-обчислювальних машин, систем і комп'ютерних мереж. Так, КК ФРН у розділі 26 "Пошкодження майна" встановлює відповідальність за протиправну зміну даних і комп'ютерний саботаж. У КК Франції в статтях 323-1, 323-2 і 323-3 глави 3 "Про посягання на системи автоматизованого опрацювання даних" розділу 2 "Про інші посягання на власність" книги 3 "Про злочини проти власності" передбачено відповідальність за незаконний доступ до системи автоматизованого опрацювання даних, перешкоджання або порушення правильності роботи такої системи та введення до неї обманним способом даних, знищення чи зміну даних, які містяться в ній.

У США питання про кримінальну відповідальність за злочини, пов'язані з комп'ютерною технікою, вирішуються інакше. В одному розділі Зводу законів США поєднані злочини, що посягають на різні об'єкти, пов'язані з використанням комп'ютерів: це шпигунство, розкрадання, незаконне одержання інформації, вимагання тощо. Відповідальність за злочини, пов'язані з комп'ютерною технікою, передбачено в параграфі 1030 "Шахрайство і подібні злочини, пов'язані з комп'ютерами" титулу 18 Зводу законів США. У цьому параграфі передбачається відповідальність за вчинення державної зради (1030 (a)(1)), посягань на власність (1030 (a)(4)) із застосуванням комп'ютерної техніки й одночасно за умисний незаконний доступ до комп'ютерної інформації (1030 (a)(5)(A) і 1030 (a)(5)(C)).

Серйозну увагу до проблеми боротьби зі злочинами у сфері використання електронно-обчислювальних машин, систем і комп'ютерних

---

[1] [97] Новый уголовный кодекс Франции /Науч. ред. Н.Ф. Кузнецова, Э.Ф. Побегайло. – М., 1994.

мереж було приділено і на міжнародному рівні. У цьому плані видаються цікавими рекомендації Ради Європи щодо вдосконалення законодавства про комп’ютерні злочини.

13 вересня 1989 року Радою Європи були прийняті рекомендації, розроблені Комітетом експертів з комп'ютерних злочинів Союзу Європи. Даний документ містить два списки дій: мінімальний і додатковий. До мінімального списку включені визначення комп'ютерних злочинів, з яких досягнуто загальної згоди й у відповідність до яких повинні бути приведені кримінальні законодавства держав-членів Союзу Європи. У додатковому списку знаходяться діяння, криміналізовані в окремих державах, але з приводу криміналізації їх усіма державами, що входять у Союз Європи, згоди досягнуто не було. Мінімальний список складають такі дії: комп'ютерне шахрайство, комп'ютерне підроблення, пошкодження комп'ютерних даних або програм, комп'ютерний саботаж, неправомірний доступ, неправомірне перехоплення, неправомірне відтворення комп'ютерних програм, неправомірне відтворення топологій напівпровідникової продукції. А додатковий список містить такі дії: зміна комп'ютерних даних або програм, комп'ютерне шпигунство, несанкціоноване використання комп'ютерів, несанкціоноване використання захищених комп'ютерних програм .[1]

У проекті Європейської конвенції про кіберзлочинність, який представлено для прийняття та підписання Комітетові Міністрів Ради Європи у червні 2001 року[1], пропонується така класифікація даних злочинів: порушення конфіденційності, цілісності та придатності комп'ютерних даних і

[1] Приводиться за [162] International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime, paragraph 191-197, http://www.ifs.univie.ac.at/~pr2qq/rew4344.html

систем (незаконний доступ, незаконне перехоплення, перекручування даних, перешкоди роботі системи, нелегальні пристрої); правопорушення, пов'язані з комп'ютером (фальсифікація даних, шахрайство пов'язане з комп'ютером); правопорушення, пов'язані зі змістом інформації (злочини, пов'язані з дитячою порнографією); порушення авторського права (незаконне відтворення та поширення за допомогою комп'ютерної системи об'єктів авторського права).

Отже, перші рекомендації Ради Європи більшою мірою відповідають американському підходу до вирішення проблеми комп'ютерних злочинів. Це можна пояснити тим, що вперше у світі комп'ютерна техніка набула значного поширення саме в США, де, так само вперше, було поставлено питання про комп'ютерні злочини. Рішення Ради Європи 1989 року являє собою запозичення цього питання без оцінки специфіки систематизації континентального законодавства. Однак, уже в проекті останнього рішення Ради Європи з комп'ютерних злочинів ми виявляємо відповідну континентальним правовим традиціям класифікацію злочинів, пов'язаних із комп'ютерною технікою. В цьому проекті виокремлюється група злочинів з якісно новим об'єктом (конфіденційність, цілісність та придатність комп'ютерних даних і систем) і визначаються злочинні посягання на традиційні об'єкти, що вчиняються з використанням комп'ютерної техніки.

Проблема цих злочинів привернула серйозну увагу і вчених. З'явилися праці, у яких робиться спроба розкрити сутність і юридичні ознаки злочинів у сфері використання комп'ютерних технологій. Особливо активізувалася ця робота в період розроблення проектів КК України та Росії. Не можна не

---

[1] [160] Draft Convention on Cyber-crime and Explanatory memorandum related thereto: final activiti report. – Prapareted by Committee of Experts on Crime in Cyber-Space (PC-CY) Submitted to European Committee on Crime Problems (CDPC) at its 50th plenary session (18 – 22 June 2001). – Secretariat Memorandym preparated by the Directorate General of Legal Affairs. – Restricted, CDPC (2001) 2 rev. 2. – Strasbourg, 20 June 2001. (Наводиться за: [24] Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО Изд-во "Юрлитинформ", 2002. – С. 134 – 139).

відзначити, що питання з розв'язання цієї проблеми, зокрема, з визначення родового об'єкту цих злочинів, їх місця в системі КК, вирішувалося по-різному.

Аналіз пропозицій щодо вдосконалення кримінального законодавства про злочини у сфері використання комп'ютерної техніки дозволяє дійти висновку, що у науковій дискусії спостерігалося переплетення американського та європейського підходів. Так, Д. Азаров[1] пропонував доповнити КК розділом, до якого включити мінімальний список таких злочинів, рекомендований Радою Європи в 1989 році. А.В. Черних[2] до розглядуваних злочинів зараховував знищення або перекручення вхідних і вихідних даних (як спосіб скоєння злочинів проти власності) та незаконне використання даних і програмного забезпечення (порушення авторського права). Ю.М. Батурін і О.М. Жодзишський[3] поділяли досліджувані злочини на дві групи: злочини, пов'язані з втручанням у роботу комп'ютерів, і злочини, що використовують комп'ютери як необхідні технічні засоби. О.П. Снегірьов і В.О. Голубєв[4] до таких злочинів відносили комп'ютерне шахрайство (злочин проти власності) і несанкціоноване копіювання (злочин проти інтелектуальної власності). Деякі автори[5] до переліку комп'ютерних злочинів додавали розкрадання комп'ютерних програм (порушення

---

[1] [1] Азаров Д. Порушення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації //Право України. – 2000. – № 12. – С. 72.

[2] [154] Черных А.В. Обеспечение безопасности автоматизированных информационных систем (уголовно-правовые аспекты) //Советское государство и право. – 1990. – № 6. – С. 116-120.

[3] [9] Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юридическая литература, 1991. – С 23-38.

[4] [127] Снегірьов О.П., Голубєв В.О. Проблеми класифікації злочинів у сфері комп'ютерної інформації //Вісник університету внутрішніх справ. Вип. 5. – Х., 1999. – С. 25-28.

[5] [47] Дубовая Л. Остерегайтесь компьютерных злоумышленников //Computer World /Киев. – № 41(62) – 1995. – 18 октября. – С. 22; [6] Баранов О.А. Проблеми законодавчого забезпечення боротьби з комп'ютерними злочинами //Інформаційні технології та захист інформації: Збірник наукових праць. – Запоріжжя: Юридичний інститут МВС України, 1998 – Вип. 2. – С. 3-13

авторського права на програмне забезпечення). М. Вертузаєв і А. Попов[1] пропонували віднести до них: використання комп'ютера для аналізу та моделювання злочинних дій; злочини, пов'язані з комп'ютерними вірусами; несанкціонований доступ до комп'ютерної інформації; несанкціоноване проникнення в інформаційно-обчислювальну мережу або масиви інформації з корисливою метою; недбалість при розробленні та створенні інформаційно-обчислювальних мереж і програмного забезпечення, яка призводить до небажаних результатів і втрати ресурсів.

Певною мірою досвід зарубіжних країн та пропозиції вчених з питань комп'ютерних злочинів були враховані в кримінальному законодавстві України: новий Кримінальний кодекс України вперше передбачив самостійний розділ про ці злочини - розділ XVI "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж".

Досліджуючи родовий об'єкт цих злочинів, насамперед цікаво порівняти КК України 1960 року і 2001 року щодо питання про їх місце у системі Особливої частини.

Стаття 198[1] "Порушення роботи автоматизованих систем" КК 1960 року була розміщена в главі IX "Злочини проти порядку управління". Отже, родовим об'єктом злочину, передбаченого цією статтею, був встановлений порядок управління – "*нормативно визначений порядок здійснення державою своєї управлінської функції, що реалізується в управлінській діяльності відповідних суб'єктів та особливому режимі функціонування її матеріальних носіїв*".[1] Відповідно, безпосереднім об'єктом порушення роботи автоматизованої системи були відносини, пов'язані з використанням автоматизованої системи, – встановлений порядок використання

[1] [20] Вертузаев М., Попов А. Предупреждение компьютерных преступлений и их расследование //Право Украины. – 1998. – №1. – С. 102.

автоматизованої системи як матеріального носія управлінської діяльності. Таке законодавче рішення не відповідало цілям кримінально-правової охорони суспільних відносин у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж, і було обставиною, що знижувала ефективність механізму кримінально-правової охорони комп'ютерної інформації. З логіки кримінального закону випливало, що не вважалося злочином знищення або перекручення комп'ютерної інформації в автоматизованій системі, яка використовується, наприклад, для зберігання, опрацювання та передавання статистичної, наукової або технічної інформації.

Цього недоліку позбавлений КК України 2001 року. Об'єднавши в одному розділі норми про відповідальність за злочини у сфері використання електронно-обчислювальних машин, їх систем та комп'ютерних мереж, він повніше відбиває соціальну значимість відносин інформатизації життя суспільства, що постійно розвиваються.

Родовий об'єкт злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж у кримінальному праві України досліджений недостатньо. Основна причина цього полягає, насамперед, у новизні норм, які передбачають відповідальність за ці злочини. У зв'язку з цим певний інтерес викликає дослідження праць російських криміналістів, присвячених даній проблемі, оскільки наукова дискусія про зміст родового об'єкта досліджуваного злочину в російському кримінальному праві почалася ще в 1996 році, коли було прийнято КК Російської Федерації, який передбачив у главі 28 злочини у сфері комп'ютерної інформації.

Аналіз визначень, які пропонувались російськими криміналістами, дозволяє зробити висновок про те, що єдиної точки зору про сутність родового об'єкта злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж не було. Одні автори вважали, що ці

---

[1] [73] Кримінальне право України: Особлива частина: Підручник для студентів юридичних вузів і факультетів /Г.В. Андрусів, П.П. Андрушко, С.Я. Лихова та ін.; За ред. П.С.

злочини "спрямовані проти тієї частини встановленого порядку суспільних відносин, яка реґулює виготовлення, використання, розповсюдження та захист комп'ютерної інформації".[1] Інші визначали родовий об'єкт досліджуваних злочинів як "право на інформацію її власника та третіх осіб".[2]

Деякі автори виходили з того, що злочини у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж являють собою посягання на системи опрацювання даних. Так, автори підручника за редакцією Б.В. Здравомислова родовим об'єктом цих злочинів вважають "права й інтереси фізичних і юридичних осіб, суспільства та держави з приводу використання автоматизованих систем опрацювання даних".[3] Близьким до наведених є визначення родового об'єкта як безпеки інформації та систем опрацювання інформації з використанням ЕОМ.[4] Найбільш повно цю позицію відображено в Коментарі до КК Російської Федерації, де родовий об'єкт цих злочинів характеризується як "сукупність відносин, пов'язаних із суспільною безпекою, що стосується виробництва, використання, розповсюдження, захисту інформації та інформаційних ресурсів, систем опрацювання інформації з використанням ЕОМ".[1]

Така позиція фактично залишилася незмінною і в літературі, виданій в 2000-2001 роках. Так, К.С. Скоромніков визначає досліджуваний родовий об'єкт як "суспільні відносини, котрі виникають у процесі комп'ютерного

Матишевського та ін. – К.: Юрінком Інтер, 1999. – С. 638.

[1] [61] Комментарий к Уголовному кодексу Российской Федерации /Отв. ред. д-р юрид. наук, проф. А.В. Наумов. – М.: Юристъ, – 1996. – С. 662.

[2] [63] Комментарий к Уголовному кодексу Российской Федерации. Издание 2-е, измененное и дополненное /Под общ. ред. Ю.И. Скуратова и В.М. Лебедева. – М. : Издательская группа Норма – Инфра М, 1998. – С. 634.

[3] [135] Уголовное право России. Особенная часть: Учебник /Отв. ред. д-р юрид. наук, проф. Б.В. Здраво-мыслов. – М.: Юристъ, 1999. – С. 350.

[4] [139] Уголовное право. Особенная часть: Учебник /Под ред. проф. А.И. Рарога. – М.: Институт международного права и экономики. Издательство "Триада, Лтд", 1997. – С. 147; Див. також: [49] Дьяконов С.В., Игнатьев А.А., Лунеев В.В., Никулин С.И. Уголовное право. – М.: Издательская группа Норма-Инфра М, 1999. – С. 287.

опрацювання інформації".[2] Це дає можливість сказати, що серед російських учених така дефініція родового об'єкту злочинів у сфері використання електронно-обчислювальних машин, систем та комп’ютерних мереж є найбільш визнаною.

Між тим, видається, що визначення безпеки автоматизованих систем опрацювання даних як родового об’єкта цих злочинів не відбиває їх сутності як посягання не з приводу автоматизованих систем, а з приводу закладеної в них інформації.

Крім того, логічним наслідком визначення як родового об’єкта досліджуваного злочину відносин, що забезпечують безпеку автоматизованих систем або відносин, які виникають у процесі комп’ютерного опрацювання інформації, буде віднесення до числа комп’ютерних і тих злочинів, котрі такими не є. Наприклад, крадіжок із банків, які вчиняються шляхом впливу на комп’ютерні системи переказу платежів і відносяться до злочинів проти власності.

Аналізуючи родовий об’єкт злочинів в сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж, не можна не сказати про те, що цінність суспільних відносин, необхідність їх охорони кримінальним законом не є незмінною категорією. Завдання суспільного розвитку на певному його етапі зумовлюють значення, цінність тих чи інших відносин, а отже, кримінально-правову заборону на їх порушення. Це положення прямо стосується питання про зміст родового об’єкта досліджуваного злочину. Як вже було відзначено у вступі, специфікою розвитку сучасного суспільства є ускладнення людської діяльності, зростання інформаційної потреби, загальна комп’ютеризація та інформатизація.

---

[1] [60] Комментарий к Уголовному кодексу Российской Федерации – М.: Проспект, 1997. – С. 595; Див. також: [116] Российское уголовное право. Особенная часть /Под ред. В.Н. Кудрявцева, А.В. Наумова. – М.: Юристъ, 1997. – С. 346-347.

[2] [125] Скоромников К.С. Компьютерное право Российской Федерации. – М.: Издательство МНЭПУ, 2000. – С. 178.

Усе це закономірно викликає розвиток певної групи однорідних суспільних відносин, які й іменуються інформаційними. Інформаційні відносини правильно визначаються О.А. Гавриловим як "об'єктивні зв'язки між окремими індивідами, їх колективами й об'єднаннями, підприємствами, державними органами й установами з приводу виробництва, розповсюдження і споживання інформації".[1]

Слід відмітити, що поняття "інформаційні відносини" зазнало серйозних змін, обумовлених самим розвитком процесу інформатизації суспільства. Так, якщо наприкінці 70-х років А.Б. Венгеров розумів під ними "відносини, які складаються у сфері управління народним господарством між працівниками, їх колективами в процесі реєстрації, збирання, передавання й опрацювання інформації",[2] то вже у 1992 році Закон України "Про інформацію" визначає їх як "відносини, що виникають у всіх сферах життя та діяльності суспільства і держави при одержанні, використанні, розповсюдженні та зберіганні інформації".[3] Така трансформація була зумовлена тим, що інформаційні відносини, зародившись як важлива складова процесу управління, проникли в усі сфери життя суспільства, так чи інакше пов'язані з інформацією.

Тому *родовим об'єктом* незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж слід вважати *інформаційні відносини у сфері використання електронно-обчислювальних машин, систем або комп'ютерних мереж.*

Суб'єктами інформаційних відносин є державні та громадські підприємства й організації, юридичні та фізичні особи, держава в цілому.

---

[1] [34] Гаврилов О.А. Курс правовой информатики: Учебник для вузов. – М.: Издательство НОРМА, 2000. – С. 25.

[2] [19] Венгеров А.Б. Право и информатика в условиях автоматизации управления (Теоретические вопросы). – М.: Юридическая литература, 1978. – С. 27.

[3] [52] Закон України "Про інформацію" від 2.11.1992 року //Закони України. Т. 4. – К., 1996. – С. 72-88.

Зміст інформаційних відносин складають права й обов'язки їх учасників, що визначаються в розділі IV Закону України "Про інформацію". Учасники інформаційних відносин мають право одержувати, використовувати, розповсюджувати та зберігати інформацію у будь-якій формі з використанням будь-яких засобів, крім випадків, заборонених законом.

До основних обов'язків суб'єктів інформаційних відносин відносяться такі: поважати інформаційні права інших суб'єктів; використовувати інформацію згідно з законом або договором (угодою); забезпечувати доступ до інформації всім споживачам на умовах, передбачених законом або угодою; зберігати інформацію в належному стані протягом встановленого терміну та надавати її іншим громадянам, юридичним особам або державним органам у передбаченому законом порядку.

Істотною ознакою інформаційних відносин є їх *предмет* – інформація. Специфіка інформації як предмета суспільного відношення полягає в тому, що вона має властивості як матеріальних, так і нематеріальних об'єктів. Це відбивається у двох взаємопов'язаних категоріях – "інформація" і "носій інформації". Співвідношення цих категорій видається можливим визначити, виходячи з характеристики такого процесу, як *фіксація інформації,* оскільки носій інформації, по суті, виступає засобом її фіксації.

Фіксація інформації пов'язана з процесом відображення. Відображення – категорія, яка позначає особливий продукт впливу однієї матеріальної системи на іншу, який являє собою відтворення в іншій формі особливостей першої системи в особливостях другої.[1] Деяка подія породжує ланцюг змін матеріальних об'єктів, що викликано наявністю в них властивості відображення. Інформація про будь-який об'єкт може бути одержана тільки шляхом матеріальної взаємодії з цим об'єктом. Усі процеси одержання,

[1] [145] Украинцев Б.С. Информация и отражение //Вопросы философии. – 1963. – № 2. – С. 27.

перетворення, зберігання та передавання інформації відбуваються за допомогою матеріальних об’єктів (носіїв інформації), стани яких і служать сигналами. При цьому необхідно, щоб об’єкт, який відображується, і об’єкт, який відображає, були в такій взаємодії, за якої зміна стану одного з них приводила б до зміни другого. Важливо також, що сигнал несе інформацію не "сам по собі", а лише тією мірою, якою певні характеристики об’єкта-сигналу пов’язані з характеристиками об’єкта, який відображається. Звідси випливає, що інформація – це не властивість самого сигналу, вона – властивість співвідношення, зв’язку між об’єктами, стан одного з яких є сигналом стану іншого.[1] Кібернетикою носій інформації визначається як "матеріал (речовина) для запису, зберігання та подальшого відтворення інформації".[2]

Таким чином, співвідношення понять "інформація" і "її носій" можна визначити так: *інформація є нематеріальним об’єктом, який включається в систему суспільних відносин за допомогою носія – матеріального об’єкта.*

Отже, в інформаційних відносинах використовуються не природні властивості матеріального предмета – носія інформації, а його специфічні, назвемо їх, *інформаційні*, властивості. Ще Г. Клаус писав, що "інформація не є чимось самостійним, чимось абсолютним, але має інформаційний характер тільки стосовно до системи, яка сприймає інформацію".[3] У цьому полягає основна відмінність інформації від інших предметів суспільних відносин. Механізм перетворення природних властивостей носія в інформаційні видається можливим описати за допомогою таких категорій, як "код" і "адресність". При цьому код являє собою характер взаємодії об’єкта, який відображається, і об’єкта, який відображає, тобто закон відповідності між станами обох об’єктів. Категорія "код" прямо пов’язана з такою властивістю

[1] [131] Тарасенко Ф.П. К определению понятия "информация" в кибернетике // Вопросы философии. – 1963. – № 4. – С. 83-84.
[2] [126] Словарь по кибернетике /Под ред. акад. В.М. Глушкова – К.: Главная редакция Украинской Советской энциклопедии. – 1979. – С. 353.
[3] [58] Клаус Г. Кибернетика и общество. – М., 1967. – С. 37. (Наводиться за: [8] Батурин Ю.М. Проблемы компьютерного права. – М.: Юридическая литература, 1991. – С. 16.).

інформації, як адресність, що передбачає наявність двох об'єктів – джерела інформації та споживача інформації (адресата). Для того, щоб одержувати інформацію, адресату повинен бути відомий код. Код "пов'язує" інформацію з носієм для її адресата. Для права важливим тут є те, *що соціально значущим у сфері правового регулювання суспільних відносин з приводу інформації буде не просто володіння суб'єктом носієм інформації, але й наявність у нього можливості "витягти" інформацію з носія*.

Важливою характеристикою інформаційних відносин є їх *соціальна значимість:* одержуючи інформацію, суб'єкт погоджує свої дії з діями інших суб'єктів, чим забезпечує їх результативність та ефективність. Інформація як необхідна умова людської діяльності робить поведінку людини усвідомленою, оскільки опосредковує зв'язки людини з людиною, людини з природою і технікою. Досить чітко соціальну значимість інформаційних відносин сформулював засновник кібернетики Норберт Вінер: "...всякий організм скріплюється наявністю засобів придбання, використання, зберігання та передавання інформації".[1] *Інформаційні суспільні відносини і являють собою засіб для одержання, зберігання та передавання інформації.* Тому вони як основа результативної, ефективної діяльності конкретної людини, врешті-решт, є необхідною умовою розвитку та стабільності суспільства.

Важливою рисою сучасних інформаційних відносин, як уже зазначалося, є зміна їх змісту. Розвиток комп'ютерних технологій спричинив якісну зміну інформаційних процесів, їх поширення, у тому числі в економічній сфері. Існує точка зору, що економіка майбутнього буде спиратися, головним чином, на інформацію і що інформація стає основним

[1] [22] Винер Н. Кибернетика или управление и связь в животном и машине. – М.: Советское радио, 1968. – С. 234.

ресурсом, який, за показником економічної ефективності, відіграватиме домінуючу роль, відтиснувши на другий план сировину й енергію.[1]

Отже, незмірно зростаюча цінність інформаційних відносин і зумовлює необхідність їх правового регулювання.

Юридичною підставою для цього є стаття 34 Конституції України, яка гарантує право кожного вільно збирати, зберігати, використовувати та розповсюджувати інформацію, щодо якої немає обмежень, встановлених законом, а також Закон України "Про інформацію" від 2 жовтня 1992 року, який визначив поняття інформації, інформаційних відносин, зміст об’єктів цих відносин, права й обов’язки їх учасників. У ньому зазначено основні принципи і напрямки державної інформаційної політики; визначено інформаційну діяльність, її напрямки та види. Також законом встановлено класифікацію інформації, її джерел і режимів доступу до неї.

Аналіз інформаційних відносин свідчить, що вони за своїм характером, змістом, відношенням до певної сфери громадського життя можуть бути різними, а тому здатні бути об’єктом різних злочинів. Родовим об’єктом злочинів, передбачених у розділі XVI КК "Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж", є тільки частина інформаційних відносин, які можна визначити як *інформаційні відносини у сфері використання електронно-обчислювальних машин, систем і комп’ютерних мереж*. Інакше кажучи, злочини, передбачені цим розділом, посягають на *певну частину* інформаційних відносин – інформаційні відносини, пов’язані із застосуванням спеціальних технічних засобів. У кримінальному законі вказуються три види таких засобів:

- електронно-обчислювальна машина (комп’ютер) – функціональний пристрій, що складається з одного або декількох взаємопов’язаних

[1] [67] Кретов Б.И. Средства массовой коммуникации – элемент политической системы общества //Социально-гуманитарные знания. – 2000. – № 1. – С. 102.

центральних процесорів і периферійних пристроїв і може виконувати розрахунки без участі людини[1];

- автоматизована система – організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей та персоналу, що здійснює цю діяльність[2];
- комп'ютерна мережа – сукупність територіально розосереджених систем опрацювання даних, засобів і (або) систем зв'язку та передавання даних, що забезпечує користувачам дистанційний доступ до її ресурсів і колективне використання цих ресурсів.[3]

Залежно від цих засобів інформаційні відносини, які є родовим об'єктом досліджуваного злочину, можуть бути поділені на три види, виокремлення яких дозволить у подальшому конкретизувати суспільну небезпечність досліджуваного злочину, його об'єктивні та суб'єктивні ознаки:

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

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

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

Перший вид цих інформаційних відносин – це найпростіша форма застосування комп'ютерної техніки для роботи з інформацією. Суб'єкти таких відносин використовують комп'ютерну техніку для виконання порівняно нескладних операцій, таких як підготування документів, проведення інженерних розрахунків, організація та робота з базами даних.

---

[1] [45] ДСТУ 2938-94. Системи оброблення інформації. Основні положення. Терміни та визначення. 01.01.96. – С. 7.

[2] [44] ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. Від 01.07.94. – С. 2.

[3] [45] ДСТУ 2938-94. Системи оброблення інформації. Основні положення. Терміни та визначення. 01.01.96. – С. 7.

Слід зауважити, що на сьогодні цей вид є домінуючим, що певною мірою можна пояснити недостатньою поширеністю в Україні комп'ютерних систем і мереж.

Використання комп'ютерних систем відноситься до більш складних інформаційних відносин. Треба зазначити, що аналіз нормативно-правових актів свідчить про невідповідність Закону України "Про захист інформації в автоматизованих системах" від 5 липня 1994 року стандарту ДСТУ 2226-93. "Автоматизовані системи. Терміни та визначення" від 01 липня 1994 року щодо визначення терміна "автоматизована система". Так, згідно з законом автоматизована система це - "система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення".[1] У названому стандарті поняття автоматизованої системи сформульовано інакше: "... організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей та персоналу, що здійснює цю діяльність".[1] На нашу думку, визначення, яке дається в законі, не зовсім вдале: керуючись ним, наприклад, не можливо відмежувати автоматизовану систему від електронно-обчислювальної машини, так як вона теж призначена для обробки даних, до її складу входять процесор, контролери, накопичувачі інформації (засоби обчислювальної техніки та зв'язку) та її необхідним елементом є програмне забезпечення. У свою чергу, визначення, яке міститься у стандарті є досить чітким і характеризує призначення автоматизованої системи – автоматизація певного виду людської діяльності. Визначення автоматизованої системи через її призначення видається більш вдалим для використання в контексті кримінально-правового дослідження, тому що дає можливість правильно вирішувати питання про соціальну значимість інформаційних відносин,

[1] [51] Стаття 1 Закону України "Про захист інформації в автоматизованих системах" // Відомості Верховної Ради України - 1994 - № 31 - Ст. 286.

пов’язаних з автоматизованими системами, а отже, і про суспільну небезпечність посягань на ці відносини. Автоматизовані системи використовуються для виконання широкого кола завдань: управління підприємством, технологічного підготування виробництва, контролю і випробування промислової продукції, управління службами життєзабезпечення підприємства тощо. Наприклад, одним із видів автоматизованих систем є система автоматизованого проектування, яка “призначена для автоматизації технологічного процесу проектування виробу, кінцевим результатом якого є комплект проектно-конструкторської документації, достатньої для виготовлення та подальшої експлуатації об’єкта проектування”.[2] Виходячи з призначення цієї системи можна зробити висновок, що суспільна небезпечність незаконного втручання в її роботу полягає: по-перше, у заподіяння шкоди інформаційним відносинам в сфері розробки продукції та, по-друге, у загрозі заподіяння шкоди відносинам, які забезпечують випуск доброякісної продукції.

Третій вид інформаційних відносин, які утворюють родовий об’єкт злочинів в сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж, пов’язаний із використанням комп’ютерних мереж, що було викликано необхідністю передавання комп’ютерної інформації на відстань. Комп’ютерні мережі бувають двох видів: локальні, які об’єднують комп’ютери в межах однієї організації, і глобальні, які забезпечують зв’язок між різними організаціями, юридичними та фізичними особами. Найвідомішою і найпоширенішою глобальною комп’ютерною мережею є INTERNET, що застосовується, в основному, для таких видів роботи з інформацією: електронна пошта; передавання файлів; віддалений доступ – можливість підключатися до віддаленого комп’ютера і працювати з ним в

[1] [44] ДСТУ 226-93 Автоматизовані системи. Терміни та визначення. 01.07.94. - С.2.
[2] [44] Там само. - С. 12.

інтерактивному режимі.[1] Комп'ютерні мережі постійно розвиваються, а інформаційні суспільні відносини в цій сфері набувають більшого значення. Наприклад, у травні 1999 року в США відбувся офіційний пуск в експлуатацію комп'ютерної мережі INTERNET-2, що забезпечує передавання інформації зі швидкістю від 4-х до 10 гігабайт на секунду. Показовим є факт: енциклопедія "Британіка" (30 книжкових томів) пересилається через INTERNET-2 за одну секунду.[2] Порушення цього виду інформаційних відносин полягає, як правило, у зменшенні ефективності роботи комп'ютерних мереж, неможливості або значній складності задоволення суб'єктами цих відносин інформаційної потреби.

Важливо відзначити, що розвиткові комп'ютерних мереж в Україні сьогодні приділяється велика увага. Про це, зокрема, свідчить прийняття спеціальних нормативно-правових актів, одним з яких є Указ Президента України від 31 липня 2000 року "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет і забезпечення широкого доступу до цієї мережі в Україні".[1]

Аналіз сутності родового об'єкта досліджуваного злочину дає змогу охарактеризувати *суспільну небезпечність посягань на нього, яка зумовлена насамперед соціальною значимістю інформаційних відносин у сучасному суспільстві: їх нормальне функціонування є необхідною умовою будь-якої людської діяльності.* Знищення або перекручення інформації призводить до порушення певної діяльності, для здійснення якої вона необхідна. Тому заподіяння шкоди інформаційним відносинам завжди призводить до порушення багатьох інших суспільних відносин.

Підвищена суспільна небезпечність незаконного втручання на сучасному етапі пов'язана також з істотними змінами в інформаційних

[1] [35] Глистер Пол. Новый Навигатор Internet. – К.: Диалектика, 1996. – С. 30-31.
[2] [66] Корж Ю. Інтернет в Україні //Вісник НАН України. – 1999. – № 1. – С. 55.

відносинах, викликаними розвитком комп'ютерної техніки. Механізм впливу технології на суспільні відносини полягає в тому, що з розвитком суспільства та постійним включенням технічних досягнень у систему людської діяльності остання все більше технологізується. Технологія стає важливою частиною самих найрізноманітніших відносин, обумовлює істотні зміни в суспільстві.[2] Наприклад, розвиток аграрно-ремісничиих технологій стимулював появу первинних форм держави, якісну зміну права та форм власності, сприяв утворенню міст. Промислове виробництво та індустріальні технології привели до формування держав нового типу, зміни соціальної структури суспільства, зростання міського населення.[3]

У свою чергу, виникнення комп'ютерної технології, внаслідок зміни кількісних характеристик інформаційних процесів (збільшення обсягів інформації, що використовується, передається, зберігається і т.ін.), сприяло *якісній зміні* інформаційних суспільних відносин. Ці зміни відбилися в тому, що *інформаційні зв'язки та інформація стали розглядатися в новій системі координат: вони стали економічними категоріями.* Частина інформаційного соціального інтересу, який є причиною діяльності, спрямованої на розповсюдження інформації, одержала нове вираження в суспільних відносинах із приводу інформації, що якісно змінилися. Інформація постає як цінний продукт і основний товар.[4] Інформаційний ресурс, тобто вся сукупність одержуваних відомостей і таких, які накопичуються в процесі розвитку науки та практичної діяльності людей для їх багатоцільового використання в суспільному виробництві й управлінні, відноситься до

---

[1][144] Указ Президента України № 928 від 31 липня 2000 року "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет і забезпечення широкого доступу до цієї мережі в Україні" // Офіційний Вісник України. - № 31. - 2000. - Ст. 1300.
[2] [113] Ракитов А.И. Философия компьютерной революции. – М.: Политиздат, 1991. - С. 16.
[3] [11] Бачинин В.А. Философия права и преступления. – Харьков: Фолио, 1999. - С.78.
[4] [148] Философия: Учебник для высших учебных заведений. – Ростов-на-Дону : Феникс, 1995. – С. 535.

найважливіших видів ресурсів, що визначають економічну, політичну та (або) військову міць їх власника.[1]

Зростання значимості інформації, процесів, пов'язаних з її виробництвом, викликало певні зміни в структурі суспільного виробництва. Так, ще наприкінці 30-х років ряд економістів пропонували розглядати суспільне виробництво як сукупність трьох основних секторів: первинного, який охоплює видобувні галузі та сільське господарство, вторинного, що включає обробну промисловість, і третинного – сфери послуг*. Зараз є підстави говорити про появу так званого "четвертинного" сектора – *інформаційного*.

Індустрія комунікації та інформації набуває в деяких країнах такої економічної ваги, що стає ключовим елементом, який заміняє в процесі створення національного продукту важку й обробну промисловість. Цікавим є прогноз розвитку цього процесу в XXI столітті, зроблений О.А. Гавриловим: "Згідно з прогнозами соціологів, XXI століття буде століттям глобальної інформатизації та комп'ютеризації всіх країн. На хвилі "електронної революції" планету покриють сотні й тисячі національних, регіональних і планетарних комп'ютерних систем і мереж. У більшості країн буде створено інформаційне товариство та інформаційну економіку. Виникне планетарна система телекомунікації".[2]

Отже, ще одним показником підвищеної суспільної небезпечності злочинів у сфері використання комп'ютерної техніки є *зростаюча економічна цінність предмета цих злочинів – комп'ютерної інформації.* Наприклад,

---

[1] [28] Воройский Ф.С. Систематизированный толковый словарь по информатике. (Вводный курс по информатике и вычислительной технике в терминах). – М.: Киберия, 1998. – С. 16.; Див. також: [82] Кураков Л.П., Смирнов С.Н. Информация как объект правовой защиты. – Гелиос, 1998. – С. 3 – 8.

* У 1940 році ця точка зору отримала систематизоване відображення у відомій роботі К. Кларка (Clark C. Conditions of Economic Progress. L., 1940).

[2] [33] Гаврилов О.А. Компьютерные технологии в правотворческой деятельности: Учебное пособие. – М.: ИНФРА М, 1999. – С. 1.

щорічні збитки від цих злочинів у США оцінюються у 100 млрд. доларів.[1] Також фахівці відзначають, що ці злочини набувають міжнародного характеру і загрожують економічним основам держав та світовій економічній системі.[2]

Слід відзначити, що небезпека досліджуваних злочинів набагато зростає, коли злочинець отримує доступ до автоматизованих систем, які використовуються у національній обороні[3], керуванні рухом повітряного або наземного транспорту, контролі над небезпечним виробництвом та інших сферах людської діяльності, які становлять підвищену небезпеку. У таких випадках незаконне втручання може призвести не тільки до значних матеріальних збитків, але й спричинити людські жертви.

Отже, стійка *тенденція зростання суспільної небезпечності комп'ютерних злочинів обумовлена прискореним розвитком науки та технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.*

Викладене дозволяє визначити такі показники суспільної небезпечності злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж:

1) досліджуваний злочин, завдаючи шкоди розвиткові інформаційних відносин, завдає шкоди великій кількості інших соціально значущих суспільних відносин;

2) досить часто злочинами у сфері використання комп'ютерної техніки завдається значна матеріальна шкода;

---

[1] [155] Черных А.В. Преступления компьютерного века // Советская юстиция. - 1987. - №11. - С 30 - 32.

[2] Див: [3] Антонов С. Компьютерные преступления в банковской сфере // Юридическая практика. –1997. – №8. – С. 7; [156] Чечко Л. "Компьютерные" хищения //Российская юстиция. – 1996. – № 5. – С. 45.

[3] См. [151] Фролов В.С., "Думающее" оружие. - М.: Знание, 1991. (Новое в жизни, науке и технике. Сер. "Радиоэлектроника и связь"; № 7). С.58 – 62.

3) втручання в роботу автоматизованих систем, використовуваних для управління системами національної оборони, рухом повітряного або наземного транспорту та ін., може призвести до заподіяння особливо тяжкої шкоди життю та здоров'ю багатьох осіб.

Із визначенням родового об'єкта злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж пов'язана ще одна проблема – проблема найменування злочинів, які посягають на цей об'єкт. Закон визначає ці злочини поняттям "злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж". У літературі все частіше зустрічається таке їх визначення, як "комп'ютерні злочини", виходячи з специфіки їх предмета.

Слід підкреслити, що це питання є актуальним, оскільки в найменуванні злочинів, поєднаних родовим об'єктом, повинна відбиватися їх сутність, основний зміст, що дало б змогу відмежовувати їх від інших та забезпечити правильну їх кваліфікацію. Відсутність чіткого визначення злочинів, передбачених у розділі XVI КК України, також значно ускладнює діяльність правоохоронних органів щодо боротьби з ними. Проведений автором аналіз звітних документів УМВС в різних областях України свідчить про те, що досить часто до злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж відносять прості крадіжки комп'ютерної техніки та виготовлення підроблених документів або фальшивих документів із використанням комп'ютерної техніки. Зрозуміло, що в таких умовах (навіть, якщо не враховувати чинників технічної оснащеності та наявності співробітників із фаховою освітою) ефективність боротьби правоохоронних органів зі злочинами, передбаченими в розділі XVI КК, знижується. Видається, що, виходячи з ознак об'єкта та предмета досліджуваних злочинів, правомірно об'єднати злочини, які посягають на інформаційні відносини у сфері використання електронно-обчислювальних

машин, систем та комп’ютерних мереж, найменуванням *"комп’ютерні злочини"* і визначити їх загальне поняття.

Не можна не звернути уваги на те, що в літературі на сьогодні термін "комп'ютерні злочини" зустрічається досить часто. Деякі автори застосовують навіть такий термін як “кіберзлочини”.[1] Але саме це поняття тлумачиться авторами по-різному - єдиного визначення понять "комп’ютерна злочинність", "комп’ютерний злочин" немає. Так, одні автори вважають, що до комп’ютерної злочинності відносяться всі протизаконні дії, при яких електронне опрацювання інформації є знаряддям їх вчинення і (або) засобом[2], або всі протизаконні діяння, предметом і засобом здійснення яких є процедури та методи, а також процес комп’ютерного опрацювання даних.[3] Пропонується і таке визначення комп’ютерних злочинів: "…усі протизаконні дії, при яких електронне опрацювання інформації було засобом їх вчинення або їх об’єктом".[4] Іноді до комп’ютерних злочинів зараховують "злочини, пов’язані з втручанням у роботу комп’ютерів, і злочини, що використовують комп’ютери як необхідні технічні засоби".[5] А.Н. Караханьян під комп’ютерними злочинами розуміє протизаконні дії, об’єктом або знаряддям вчинення яких є електронно-обчислювальні машини.[6] В.О. Голубєв вважає, що основна класифікуюча ознака належності злочинів до розряду

---

[1] [39] Голубєв В.О. Теоретично-правові проблеми боротьби з комп’ютерною злочинністю // Вісник Запорізького юридичного інституту. –1999. – № 3. – С. 52 – 60. (с. 52 – 60)

[2] [57] Калюжный Р.А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект): Автореф. дисс. … д-ра юрид. наук: 12.00.02 /АН Украины, Институт государства и права им. В.М. Корецкого. – К., 1992. – С. 14.

[3] [1] Азаров Д. Порушення роботи автоматизованих систем – злочини у сфері комп’ютерної інформації //Право України. – 2000. – № 12. – С. 72.

[4] [16] Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп’ютерна злочинність: Навчальний посібник. – К.: Атіка, 2002. – С. 65.

[5] [9] Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юридическая литература, 1991. – С. 11.

[6] [106] Полевой Н.С. и др. Правовая информатика и кибернетика: Учебник. – М.: Юридическая литература, 1993. – С. 243.

комп’ютерних це “використання засобів комп’ютерної техніки”[1], В. Лісовий визначає цю ознаку інакше: “електронна обробка інформації”, незалежно від того на якій стадії злочину вона застосовувалася.[2] Пропонується і така дефініція комп’ютерних злочинів: “передбачені кримінальним законом суспільно небезпечні діяння, у яких машинна інформація є або засобом, або об’єктом злочинного посягання”.[3]

Деякі автори дають більш широке визначення. Так, П.Д. Біленчук і М.А. Зубань вважають, що комп’ютерна злочинність – це "суспільно небезпечна діяльність або бездіяльність, яка здійснюється з використанням сучасних технологій і засобів комп’ютерної техніки з метою завдання шкоди майновим або суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадським організаціям і громадянам, а також правам особи".[1] Виходячи з такого розуміння комп’ютерної злочинності, комп'ютерним злочином може визнаватися будь-який злочин – розкрадання, шпигунство, незаконне збирання відомостей, які становлять комерційну таємницю, і т.ін., якщо він вчиняється з використанням комп’ютера. Таке розуміння комп’ютерних злочинів видається неправильним, оскільки не дозволяє відбити їх сутність, специфіку та відрізнити від інших злочинів, у яких комп’ютер є лише знаряддям, засобом або предметом.

Водночас виникає ще одне дуже важливе питання. Якщо в усьому світі з використанням комп’ютерів вчиняються крадіжки з банків на астрономічні суми, викрадаються важливі державні таємниці, доводяться до банкрутства

---

[1] [38] Голубєв В.О. Правові проблеми захисту інформаційних технологій // Вісник Запорізького юридичного інституту. –1997. – № 2. – С. 39 – 40.

[2] [84] Лісовий В. “Комп’ютерні” злочини: питання кваліфікації // Право України. – 2002. – № 2. – С. 87.

[3] [14] Бидашко Е.А., Волкова Н.Л. Компьютерные преступления: миф или реальность? // Нуковий вісник Дніпропетровського юридичного інституту МВС України. – 2001. – № 1 (14). – С. 161.

великі компанії, то чому ж санкції статей глави XVI КК України настільки невеликі: основне покарання – до п’яти років позбавлення волі? Відповідь досить проста: перелічені вище суспільно небезпечні діяння не є комп’ютерними злочинами. Такі діяння, незважаючи на використання для їх вчинення комп’ютерної техніки, залишаються державною зрадою, шпигунством, крадіжкою, шахрайством, незаконним збиранням відомостей, що становлять комерційну таємницю і т.ін. Засіб не змінює суті злочину, тому правильною видається пропозиція В.В. Голіни і В.В. Пивоварова, висловлена ними ще під час обговорення проекту КК України, про внесення до переліку обставин, що обтяжують покарання, такої ознаки, як "вчинення злочинів із використанням засобів електронно-обчислювальної техніки".[1]

Доречно навести такий приклад. Як відомо, виготовлення підроблених грошових купюр за допомогою сучасних кольорових ксероксів, не зважаючи на підвищення суспільної небезпечності, не змінило кваліфікації цих діянь: винні притягувалися та продовжують притягуватися до кримінальної відповідальності за статтями про виготовлення, зберігання, придбання, перевезення, пересилання, ввезення в Україну з метою збуту підроблених грошей (ст. 79 КК України 1960 р., ст. 199 КК КУкраїни 2001 р.), так само як і ті, хто використовував для підроблення фототехніку або звичайні олівці, фарби та лезо бритви. Комп’ютерна техніка дозволяє до досконалості довести процес виготовлення підроблених документів: перенесені з оригіналу печатки, підписи, інші реквізити практично ідентичні. Для встановлення підробки необхідне проведення висококваліфікованої криміналістичної експертизи, але це не означає, що такого роду підроблення документів

[1] [15] Біленчук П.Д., Зубань М.А., Комп’ютерні злочини: соціально-правові та кримінолого-криміналістичні аспекти: Навчальний посібник. – К.: Українська академія внутрішніх справ, 1994. – С. 6.; [159] Шилан Н.Н., Кривонос Ю.М., Бирюков Г.М. Компьютерные преступления и проблемы защиты информации: Монография – Луганск: РИО ЛИВД, 1999. – С. 9.

потребує особливої, відмінної від існуючої кваліфікації. Висновок може бути тільки один: *модифікація знарядь і засобів скоєння злочину, використання з цією метою досягнень науково-технічного прогресу не змінює тих відносин, на які він посягає, а тому не можуть впливати на його кваліфікацію.* Підвищення суспільної небезпечності такого роду діянь потребує лише відповідної оцінки в питанні про межі кримінальної відповідальності та покарання.

Сказане зовсім не означає, що немає і не може бути комп'ютерних злочинів, як, наприклад, вважає Ю.М. Батурін. На його думку, комп'ютерних злочинів як особливої групи злочинів у юридичному розумінні не існує, однак, відмічаючи безсумнівну модифікацію традиційних злочинів з причини залучення до них комп'ютерної техніки, автор гадає, що правильніше було б говорити лише про комп'ютерні аспекти злочинів, не виділяючи їх в уособлену групу.[2]

Аналізуючи це питання, слід перш за все розмежовувати терміни "комп'ютерні злочини" і "злочини, пов'язані з комп'ютерною технікою". Можна погодитися з В.В. Вєховим, який пропонує давати різні визначення комп'ютерних злочинів з точки зору кримінально-правової охорони і з точки зору криміналістичної.[3] Очевидно, що остання група більш широка. Саме її можна визначати як діяння, в яких комп'ютер є предметом, знаряддям або засобом скоєння злочину. Виокремлення цієї групи має значення для криміналістики з огляду на специфіку методики розслідування. Але в кримінальному праві такий поділ видається помилковим.

---

[1] [36] Голина В.В., Пивоваров В.В. Проблемы компьютерной преступности //Фінансова злочинність: Зб. матеріалів міжнар. наук.-практ. семінару [Харків, 12-13 лютого 1999 р.] /[Редкол.: Борисов В.І. (голов. ред.) та ін.]. – Х.: Право, 2000. – С. 64-65.

[2] [8] Батурин Ю.М. Проблемы компьютерного права. – М.: Юридическая литература, 1991. – С. 129.

[3] [21] Вехов В.В. Компьютерные преступления: Способы совершения и раскрытия /Под ред. акад. Б.П. Смагоринского. – М.: Право и Закон, 1996. – С. 23-24.

Комп'ютерні злочини - це новий вид суспільно небезпечних діянь, а тому їх визначення необхідно давати з урахуванням ознаки, яка є основою діючої класифікації злочинів. Як відомо, класифікація – це розподіл предметів будь-якого роду на взаємопов'язані класи згідно *з найістотнішими* ознаками, властивими предметам даного роду. Як вірно зазначає М.В. Салтевський "у кримінальному праві та криміналістиці вид злочину називають не за зсобом (знаряддям) вчинення злочину, а за видом злочинної діяльності".[1] Найістотнішою ознакою злочинів, їх якісною характеристоко є об'єкт. Класифікація за родовим об'єктом – це системоутворюючий фактор сукупності норм Особливої частини КК. Тому визначення комп'ютерних злочинів повинне конструюватися на основі специфічних ознак їх родового об'єкта.

Визначивши суспільні відносини, яким завдається шкода в результаті вчинення комп'ютерних злочинів, видається можливим сформулювати й саме поняття "комп'ютерні злочини": це **суспільно небезпечні, винні, кримінально карані, діяння, що завдають шкоди інформаційним відносинам, засобом забезпечення яких є електронно-обчислювальні машини, системи або комп'ютерні мережі.**

1.3. Безпосередній об'єкт незаконного втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем та комп'ютерних мереж

Загальновизнаним в кримінальному праві є положення, що в будь-якому складі злочину безпосередній об'єкт є частиною родового об'єкта, а тому відношення, яке виступає безпосереднім об'єктом, повинне

[1] [118] М.В. Салтевський Основи методики розслідування злочинів, скоєних з використанням ЕОМ. Навчальний посібник. – Харків: Нац. Юрид. Акад. України, 2000. – С. 4.

охоплюватися сукупністю тих суспільних відносин, які складають родовий об’єкт.

Як вже було визначено, родовим об’єктом злочинів, передбачених у розділі XVI КК, виступає сукупність інформаційних відносин у сфері використання електронно-обчислювальних машин, систем та комп’ютерних мереж. Ці відносини не є однорідними і включають різні види, тому завдання дослідження безпосереднього об’єкта незаконного втручання полягає, насамперед, у тому, щоб виділити такий за змістом вид інформаційних відносин, який завжди страждає від його вчинення і, отже, може розглядатися як безпосередній об’єкт. Це дозволить не тільки розкрити специфіку цього злочину, його суспільну небезпечність, але й відмежувати від суміжних злочинів, які посягають на той самий родовий об’єкт.

Незважаючи на те, що склад незаконного втручання є відносно новим, у літературі робилися спроби визначити його безпосередній об’єкт. Єдиної думки з цього питання немає. А.М. Ришелюк пропонує вважати цим об’єктом нормальну роботу комп’ютерів і комп’ютерних мереж, а також встановлений порядок використання електронно-обчислювальних машин і комп’ютерних мереж.[1] Поділяючи наведену позицію, А.В. Загіка розуміє безпосередній об’єкт незаконного втручання як "відносини у сфері безпеки користування речовими та інтелектуальними засобами обчислювальної техніки".[2] Здається, що такі визначення не відповідають специфіці незаконного втручання і містять недолік, на який зверталася увага при розгляді родового об’єкта незаконного втручання: суспільні відносини, котрим завдається шкода при скоєнні цього злочину, складаються не з приводу комп’ютерної техніки або безпеки її використання, а з приводу інформації, що опрацьовується

[1] [91] Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001 року /За ред. М.І. Мельника, М.І. Хавронюка. – К.: Каннон, 2001. – С. 902.

[2] [141] Уголовный кодекс Украины. Комментарий /Под ред. Ю.А. Кармазина и Е.Л. Стрельцова. – Х.: ООО "Одиссей", 2001. – С. 747.

електронно-обчислювальними машинами, системами та комп'ютерними мережами.

Значний інтерес становить позиція ряду вчених про те, що об'єктом злочинів у сфері використання ЕОМ, систем і комп'ютерних мереж є право власності на інформацію. Певною мірою ця точка зору грунтувалася на тому, що в Законі України "Про інформацію" при характеристиці інформаційних відносин називалася така категорія, як "право власності на інформацію" (ст. 38).[1] Це положення викликало серйозну дискусію насамперед серед цивілістів. Однак видається, що позиції цивільного та кримінального права в самому визначенні таких правових категорій, як "власність", "право власності", не повинні розходитися. Не може по-різному розумітися і така категорія, як "власність на інформацію". Одним із аргументів вирішення цього питання може служити те, що ефективність цивільно-правових інститутів багато в чому забезпечується наявністю санкцій за їх порушення. У ряді випадків, залежно від соціальної значимості цивільно-правового відношення, його охорона забезпечується нормами закону про кримінальну відповідальність. Так, наприклад, забезпечується ефективність цивільно-правового інституту власності на річ. Виходить, якщо в кримінальному праві під відносинами власності на інформацію розуміти щось інше, ніж у цивільному, то вони не будуть мати належний рівень правової охорони. Саме це й зумовлює інтерес до дискусії цивілістів і теоретиків права щодо поняття суспільних відносин власності на комп'ютерну інформацію.

Деякі вчені вважають недоцільним застосування такої категорії, як "власність на інформацію". Так, О.А. Гаврилов відзначає, що "інформація як така не може бути об'єктом права власності, оскільки вона є абстрактним ідеальним об'єктом, між тим право власності цивільний закон пов'язує з

[1] [52] Закон України "Про інформацію" від 2.11.1992 року //Закони України. Т. 4. – К., 1996. – С. 72-88.

матеріальними, речовими об’єктами, із речами".[1] Подібної точки зору дотримується і Л.К. Терещенко, який доходить висновку, що класична "тріада" правомочностей власника, котрий має абсолютне право на річ, не може застосовуватися відносно до інформації. До неї не можна застосовувати правомочність "володіння", оскільки нереально фізично володіти ідеальними об’єктами; "користування" – оскільки інформація може знаходитися одночасно в користуванні великої кількості осіб; "розпоряджання" – оскільки, відчужуючи право на її використання, продавець не позбавляється можливості її подальшого використання.[2]

Ряд авторів, навпаки, наголошують на правильності застосування для регулювання інформаційних суспільних відносин поняття "право власності на річ". Наприклад, В. Кузнєцов гадає, що комп’ютерну інформацію[*] можна визнати предметом матеріального світу[3] і наводить такі аргументи. *По-перше*, відмічаючи, що згідно з законодавством до інформації можна застосовувати повноваження власника і що неможливо застосувувати зазначені повноваження до нематеріальних предметів, дослідник робить висновок, що інформація – це "самостійне явище, яке фактично дорівнюється до матеріальної речі". *По-друге,* він пропонує вважати річчю не всю інформацію, а лише комп’ютерну інформацію з обмеженим доступом.

---

[1] [32] Гаврилов О.А. Информатизация правовой системы России. Теоретические и практические проблемы. – М., 1998. – С. 61; Див також [33] Гаврилов О.А. Компьютерные технологии в правотворческой деятельности: Учебное пособие. – М.: ИНФРА М, 1999. – 108 с.

[2] [133] Терещенко Л.К. Информация и собственность //Защита прав создателей и пользователей программ для ЭВМ и баз данных (комментарий российского законодательства). – М., 1996. – С. 3-11; Наводиться за: [120] Северин В.А. Правовое регулирование информационных отношений //Вестник МГУ. Серия 11. Право. – 2000. – № 5. – С. 24.

[*] Властивості комп’ютерної інформації варіативніші за властивості інформації, яка міститься на інших носіях (наприклад, на папері), поглинають їх, тому викладення й обговорення проблем правової регуляції суспільних відносин з приводу комп’ютерної інформації цілком можна використовувати для обговорення проблем правової регуляції інформації взагалі.

[3] [81] Кузнєцов В. Комп’ютерна інформація як предмет крадіжки //Право України. – 1999. – № 7. – С. 86.

Досить поширеною є третя точка зору. Її, зокрема, дотримується С.І. Семилєтов. Він доходить висновку, що інформацію некоректно вважати об’єктом права власності, оскільки вона належить до нематеріальних предметів права. Однак гадає, що відносини з приводу інформації слід регулювати за допомогою інституту, який нагадує авторське право. Як в авторському праві твір не є предметом права інтелектуальної власності, а власність на матеріальний носій твору не пов’язана з авторським правом, так і право на розповсюдження і використання інформації, на його думку, не пов’язане з правом на матеріальний носій .[1]

Дослідження різних точок зору дозволяє зробити ряд висновків, які мають важливе значення для вирішення питань про безпосередній об’єкт незаконного втручання.

1. Аналізуючи наведені положення про неможливість застосування терміна "право власності" для регулювання інформаційних відносин, можна погодитися з тим, що інформація не є річчю, а отже, до неї неможливо застосувати поняття "право власності на річ", але це зовсім не означає, що поняття "право власності" неможливо застосувати до інформаційних відносин.

2. Регулювання інформаційних відносин за допомогою інституту права власності на річ видається неправильним. Наведений В. Кузнєцовим аргумент про те, що, якщо законодавець застосовує відносно інформації такі поняття, як "володіння", "користування" і "розпоряджання", то інформація є річчю матеріального світу та предметом права власності на річ, не є слушним. Такі міркування нагадують дискусію цивілістів про термін "інтелектуальна власність". Є.А. Суханов називає його "результатом непорозуміння", відмічаючи, що його використання для позначення виключних прав автора є "умовним, таким, що являє собою відому данину деяким стандартам і

[1] [121] Семилетов С.И. Информация как особый нематериальный объект права // Государство и право. – 2000. - №5. - С. 67-74

традиціям". За автором визнаються особливі авторські права, які забезпечують його інтерес як творця, але не як особи, що володіє річчю.[1] Ще на початку XX століття Т.Ф. Шершеневич відзначав, що "поширювати поняття про речові права на права, які не мають своїм об'єктом речі, видається теоретично незручним. Порядок виникнення, переходу, припинення речових прав розрахований саме на матеріальний їх зміст, і тому поширення цих правил на цілком іншу галузь може створити небажане змішування понять у теорії та практиці".[2] Така ж ситуація спостерігається зараз і в правовому регулюванні інформаційних відносин. Застосування відносно до інформації термінів "володіння", "користування" і "розпоряджання" зовсім не означає, що інформація дорівнюється до речі й інформаційні відносини регулюються правом власності на річ.

Необхідно також відзначити, що віднесення інформації до матеріальних предметів права та пропозиції забезпечити правове регулювання інформаційних відносин на основі права власності на річ суперечать сформованим наукою уявленням про інформацію. Ще Н. Вінер підкреслював, що "інформація – це інформація, не матерія і не енергія".[3] А.Б. Венгеров, досліджуючи правові аспекти інформатики, виділяв таку властивість інформації, як її самостійність стосовно свого носія.[4] Крім того, слід враховувати, що, коли інформація ототожнюється з носієм, то і право власності на інформацію ототожнюється з володінням, користуванням і розпоряджанням не інформацією, а її носієм, тобто з правом власності на річ. Можливість же застосування для регулювання суспільних відносин з приводу комп'ютерної інформації права власності на річ досить справедливо піддано критиці в літературі.

---

[1] [128] Суханов Е.А. Курс лекций по гражданскому праву. – М.: 1987. – С. 153.
[2] [158] Шершеневич Т.Ф. Учебник русского гражданского права (по изданию 1907 г.). – М.: Фирма "Спартак", 1995. – С. 254-255.
[3] [23] Винер Н. Кибернетика. – М., 1983. – С. 208.
[4] Наведено за: [8] Батурин Ю.М. Проблемы компьютерного права. – М.: Юридическая литература, 1991. – С. 14.

Так, А.Б. Венгеров пише, що інформація істотно відрізняється від речових об'єктів тим, що при передаванні вона зберігається у суб'єкта, який її передає, тому юридично передавання інформації не можна дорівнювати до передавання речей.[1]

Російські вчені, порівнюючи знищення або пошкодження комп'ютерної інформації зі знищенням або пошкодженням майна, відмічають два основні моменти:

- ці злочини посягають на різні предмети[2];

- інформація не має властивостей предмета злочинів проти власності, зокрема фізичної властивості.[3]

Неодноразово в літературі підкреслювалося, що і норми про розкрадання майна не можна застосовувати для кваліфікації випадків копіювання комп'ютерної інформації.[4]

Аналогічний підхід спостерігається і в країнах далекого зарубіжжя. У розділі 3 Закону про неправомірне використання комп'ютерів (Computer Misuse Act 1990) Сполученого Королівства Великобританії та Північної Ірландії сказано, що перекручення комп'ютерної інформації не є пошкодженням комп'ютера або носія інформації, за винятком випадків, коли порушується їхня фізична цілісність, і не повинне кваліфікуватися за законом про заподіяння шкоди майну (Criminal Damage Act 1971).[5] Цю особливість

---

[1] [18] Венгеров А.Б. Категория "информация" в понятийном аппарате юридической науки //Советское государство и право. – 1977. – № 10. – С. 70-71.

[2] [139] Уголовное право. Особенная часть: Учебник /Под ред. проф. А.И. Рарога. – М.: Институт международного права и экономики. Издательство "Триада, Лтд", 1997. – С. 231.

[3] [61] Комментарий к Уголовному кодексу Российской Федерации /Отв. ред. д-р юрид. наук, проф. А.В. Наумов. – М.: Юристъ. – 1996. – С. 662-663.

[4] [154] Черных А.В. Обеспечение безопасности автоматизированных информационных систем (уголовно-правовые аспекты) //Советское государство и право. – 1990. – № 6. – С. 118; [10] Батурин Ю.Н., Жодзишский А.М. Компьютерные правонарушения: криминализация, квалификация, раскрытие //Советское государство и право. – 1990. – № 12. – С. 87-88.

[5] [165] Stein Schjolberg, Chief Judge Moss byrett, Norway "The Legal Framework – Unauthorized Access to Computer Systems. Penal Legislation in 37 Countries", http://www.mossbyrett.of.no/legal.html.

інформації відмічено і в Рекомендаціях ООН по боротьбі з комп'ютерними злочинами та їх попередженню, де зафіксовано, що при дослідженні питань, пов'язаних із кримінально-правовим захистом комп'ютерної інформації, необхідно враховувати значну відмінність між правовим захистом власника матеріальних і нематеріальних (інформаційних) об'єктів, а також те, що правовий режим інформації, а отже і вимоги до організації її охорони включають не тільки економічні характеристики об'єкта (як при організації охорони майна), а й питання, пов'язані зі змістом інформації.[1]

Отже, правове регулювання суспільних відносин з приводу інформації за допомогою інституту права власності *на річ* не випливає із сутності інформації і є в правовому відношенні необґрунтованим. Правовий інститут власності на річ може бути застосований тільки до матеріальних носіїв інформації. Але оскільки інформація, як відзначалося раніше, не тотожна носію, то і правове регулювання відносин власності на носій не тотожне правовому регулюванню відносин власності на інформацію. На підтвердження того, що регламентація суспільних відносин з приводу інформації за допомогою інституту права власності на реч є неефективною, можна також зіставити зміст правомочності розпоряджання річчю та розпоряджання інформацією: розпоряджання інформацією набагато ширше за розпоряджання її носієм (річчю).

3. Розглядаючи третю точку зору, щодо можливості регулювання інформаційних відносин за допомогою інститутів інтелектуальної власності, не можна не відзначити, що таке регулювання не відбиває їх специфіки, зокрема, особливостей предмета цих відносин – інформації, що нерозривно пов'язана з носієм.

Таким чином, розуміння інформації як нематеріального або матеріального предмета саме по собі не забезпечує вирішення завдань

[1] [162] International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime, paragraph 86-87, http://www.ifs.univie.ac.at/~pr2qq

правового регулювання й охорони суспільних відносин у цій сфері. Це пояснюється тим, що інформація та інформаційні відносини не укладаються в наявні на сьогодні правові механізми. Використання для регулювання цих відносин права власності на річ не враховує того, що даний правовий інститут орієнтований на відносини щодо використання природних властивостей матеріальних об'єктів (у досліджуваних відносинах використовуються інформаційні властивості носія). Метою ж інституту інтелектуальної власності є захист прав автора твору, а тому і цей інститут не буде забезпечувати захист інтересів особи, яка володіє інформацією, але *не є її автором.*

Враховуючи викладені характеристики й специфіку сучасних інформаційних відносин та інформації як предмета правового регулювання, інформаційні відносини пропонується регулювати та забезпечувати їх кримінально-правову охорону за допомогою *специфічного інституту права власності на інформацію.*

Складність інформації як предмета права зумовлює відому обережність у поширенні на неї правовідносин власності. Однак, незважаючи на безсумнівну специфіку, інформація поза відносинами власності первісно не може стати об'єктом правової охорони, оскільки не може існувати поза суб'єктом, який її розробив, придбав, одержав право користування. Кримінально-правова охорона інформації орієнтована на охорону цих суб'єктивних прав. *Ось чому застосування для регламентації суспільних відносин з приводу інформації такої фундаментальної правової категорії, як власність, дозволить створити правову структуру, що відповідатиме сучасним тенденціям розвитку цих відносин, дати в подальшому адекватну правову оцінку новим явищам у цій сфері.*

/rew4344.html.

Інформація як предмет права власності являє за своїм змістом *сприймані і використовувані людиною відомості про об'єктивний світ і процеси, що протікають у ньому.*

Зміст відносин власності на інформацію – це класична сукупність повноважень власника, зміст яких визначається з урахуванням специфіки їх предмета – інформації.

Як уже відзначалося, інформація не існує без носія і "сама по собі" у систему суспільних відносин включена бути не може. Необхідною передумовою власності на інформацію є володіння її носієм. Виходячи з цього, доцільно володіння як елемент права власності на інформацію визначати таким чином: *наявність у особи права та можливості володіння носієм інформації.*

Право користування являє собою наявність у особи права та можливості задовольняти за допомогою інформації свої потреби. При здійсненні права користування річчю потреба задовольняється шляхом використання фізичних властивостей предмета, що й закріплено в механізмі правового регулювання цих відносин (праві власності на річ). Застосування такого ж механізму для регулювання відносин з приводу інформації, як ми зазначали вище, не забезпечує їх адекватного правового відображення. Задоволення інформаційної потреби здійснюється шляхом використання інформаційних властивостей носія. Використання при створенні механізму правового регулювання відносин з приводу інформації описаної специфіки інформації як предмета правового регулювання дозволяє усунути ототожнення інформації з її носієм. Отже, право користування інформацією можна визначити таким чином: *наявність у особи права та можливості використовувати інформацію, яка міститься на носії, для задоволення своєї інформаційної потреби.*

Якщо право володіння є основою власності на інформацію, а право користування відображає особливості задоволення потреб в інформаційній

сфері, то право розпоряджання являє собою форму реалізації цих відносин і відображає соціальний інтерес розповсюдження інформації. Отже, право розпоряджання інформацією слід визначати таким чином: *наявність у особи права та можливості дозволяти доступ до інформації, яка міститься на його носії, іншим особам; змінювати інформацію, яка міститься на носії; визначати долю носія.*

Право дозволяти доступ полягає в тому, що власник може надати можливість іншим особам використовувати інформацію, яка міститься на його носії. Дозволяючи доступ, власник може обмежити його за колом осіб і характером використання інформації. За колом осіб, яким власник дозволяє використовувати інформацію, доступ буває обмеженим і необмеженим. До обмеженого доступу відносяться випадки надання доступу до таємної інформації (державна таємниця, комерційна таємниця, військова таємниця тощо) і надання платного доступу до інформації; до необмеженого - випадки безкоштовного надання доступу до інформації або обов’язкового надання доступу до інформації.

При цьому у випадках платного надання доступу до інформації та необмеженого доступу особа, яка одержала інформацію, сама стає новим власником інформації.

Обмеження використання одержаної інформації матиме місце в разі надання доступу до інформації з обмеженим доступом. У такому випадку встановлюються спеціальні вимоги до володіння (володіння носієм), використання та розпоряджання одержаною інформацією.

Таким чином, право власності на інформацію - це *сукупність права та можливості особи: володіти носієм інформації; використовувати інформацію, яка міститься на ньому, для задоволення своєї інформаційної потреби; дозволяти іншим особам використовувати інформацію, яка міститься на його носії, змінювати її, визначати долю носія.*

Викладені положення повною мірою відповідають змісту інформаційних відносин та інформації як їх предмета. Специфіка інформаційних відносин, яка полягає в тому, що, одержуючи інформацію, суб'єкт погоджує свої дії з діями інших осіб, процесами, котрі відбуваються в об'єктивному світі, знаходить своє відображення в запропонованому визначенні інформації і такому елементі права власності на неї, *як користування.* Тенденції розвитку інформаційних відносин в економічній площині враховуються в *праві розпоряджання*, а та особливість інформації, що "сама по собі" вона не може бути включена до системи суспільних відносин, знаходить вирішення у *праві володіння*.

Таким чином, безпосереднім об'єктом даного злочину є *охоронювана кримінальним законом структурно організована та нормативно врегульована система соціально значущих відносин власності на комп'ютерну інформацію, яка забезпечує свободу реалізації права кожного учасника на задоволення інформаційної потреби.*

Таке визначення безпосереднього об'єкта незаконного втручання в роботу електронно-обчислювальних машин досить повно відображує механізм заподіяння шкоди суспільним відносинам власності на комп'ютерну інформацію, який полягає в порушенні, позбавленні або обмеженні реалізації власником інформації повноважень володіння, розпоряджання, користування нею.

Виходячи зі специфіки інформації, безпосередній об'єкт злочину як право власності на комп'ютерну інформацію може виступати у двох видах: відносини власності на відкриту комп'ютерну інформацію та відносини власності на комп'ютерну інформацію з обмеженим доступом.

Дослідження об'єкта незаконного втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж показує, що, крім розглянутого основного об'єкта, у даному складі можливі й додаткові факультативні об'єкти. Видається, що такими об'єктами можуть бути в

конкретних злочинах відносини в різних сферах діяльності людини, пов’язані з використанням електронно-обчислювальних машин, систем і комп’ютерних мереж. Заподіюючи шкоду відносинам власності на комп’ютерну інформацію, злочинець завдає або ставить під загрозу завдання шкоди тим суспільним відносинам, для інтенсифікації яких застосовується комп’ютерна техніка. Такими можуть бути відносини адміністративного управління, управління виробництвом, відносини, пов’язані з забезпеченням безпеки руху, відносини щодо розроблення нових технологій тощо.

Так, наприклад, у 1971 році американська залізнична компанія "Нью-Йорк Пенн Централ Рейлроуд" виявила зникнення 200 вагонів із цінними вантажами, які їй належали. Під час перевірки з’ясувалося, що постраждали й інші транспортні фірми. Вартість окремих вагонів перевищувала 60 тис. доларів. Розслідуванням було встановлено, що злочинці перекрутили інформацію в ЕОМ, яка керує процесом відправлення вагонів.[1] У даному випадку, крім основного об’єкта – права власності на комп’ютерну інформацію, постраждали такі додаткові об’єкти, як право власності транспортних компаній на вантажі та безпека руху залізничного транспорту.

На початку 80-х років шляхом перекручення інформації в комп’ютері, який керує роботою конвейєра Волзького автомобільного заводу, була на певний час зупинена його робота.[2] Додатковим об’єктом у цьому випадку були суспільні відносини управління виробничими процесами.

У 1992 році мало місце умисне порушення роботи автоматизованої системи управління Ігналінської АЕС.[3] Тут у якості додаткових об’єктів виступали відносини управління технологічними процесами та відносини забезпечення безпеки життя та здоров’я робітників.

---

[1] [37] Голубев В.В., Дубров П.А., Павлов Г.А. Компьютерные преступления и зашита информации в вычислительных системах //Защита информации. – М.: Знание, 1990. – С. 4

[2] [7] Батурин Ю.М. Компьютерное право: краткий реестр проблем //Советское государство и право. – 1988. – № 8. – С. 63-74

[3] [87] Ляпунов Ю., Максимов В., Ответственность за компьютерные преступления //Законность. – 1997. – № 1 – С. 45.

Таким чином, додатковий об’єкт, не будучи обов’язковим, підлягає обов’язковому встановленню, оскільки дозволяє правильно оцінювати суспільну небезпечність скоєного комп’ютерного злочину та є необхідною умовою призначення справедливого покарання.

1.4. Предмет комп’ютерних злочинів

Серед великої кількості підходів до визначення предмета злочину правильною видається точка зору В.Я. Тація, який визначає предмет злочину як "будь-які речі матеріального світу, із певними властивостями яких кримінальний закон пов’язує наявність у діяннях особи ознак конкретного складу злочину".[1]

Перебуваючи в нерозривному зв’язку з об’єктом злочину, дозволяючи в багатьох випадках правильно визначити його зміст, механізм завдання йому шкоди, а також суспільну небезпечність злочину, предмет виступає факультативною ознакою в загальному понятті складу злочину і в різних складах злочину має різне правове значення. У науці кримінального права загальновизнано, що в залежності від визначення в законі складу злочину предмет може відігравати три різні ролі:

1) обов’язкової ознаки;
2) кваліфікуючої ознаки;
3) ознаки, яка пом’якшує або обтяжує покарання.

У досліджуваному складі злочину предмет передбачений як *обов’язкова ознака*, тобто його відсутність виключає склад незаконного втручання. При цьому закон називає три предмети незаконного втручання:

- комп’ютерна інформація;
- носій комп’ютерної інформації;

[1] [132] Таций В.Я. Объект и предмет преступления в советском уголовном праве. – Х.: Вища школа: Изд-во при ХГУ, 1988. – С. 47

- комп’ютерний вірус.

Між тим у літературі висловлюється думка, що предметом у цьому злочині є й автоматизовані електронно-обчислювальні машини, їх системи та комп’ютерні мережі.[1] Висловлюються й інші погляди на цю проблему. Наприклад, Н. Розенфельд до предмета незаконного втручання відносить не тільки електронно-обчислювальні машини, їх системи, комп’ютерні мережі, комп’ютерну інформацію, її носії, але й захисні системи електронно-обчислювальних машин, їх систем, комп’ютерних мереж, комп’ютерної інформації та носіїв такої інформації. Вона обгрунтовує, що програмно-математичні й апаратно-програмні засоби в програмній частині захисту електронно-обчислювальних машин, їх систем та комп’ютерних мереж належать до різновиду комп’ютерної інформації, у свою чергу, апаратні й апаратно-програмні заходи захисту в апаратній частині – до технічного устаткування електронно-обчислювальних машин, систем та комп’ютерних мереж.[2] Такі точки зору не можна визнати правильними за двох причин: по-перше, вони суперечать диспозиції статті 361 КК України; по-друге, визнання електронно-обчислювальних машин, систем і комп’ютерних мереж предметами незаконного втручання не відповідає поняттю предмета злочину, оскільки вони не є тими речами матеріального світу, з приводу яких вчиняється цей злочин і які є інтересом, що спонукав особу до незаконного втручання. Тому електронно-обчислювальні машини, системи та ком’ютерні мережі виступають лише засобами незаконного втручання, які забезпечують посягання на об’єкт.

---

[1] Див.: [141] Уголовный кодекс Украины. Комментарий /Под ред. Ю.А. Кармазина и Е.Л. Стрельцова. – Х.: ООО "Одиссей", 2001. – С. 747; [91] Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001 року /За ред. М.І. Мельника, М.І. Хавронюка. – К.: Каннон, 2001. – С. 902; [90] Науково-практичний коментар до Кримінального кодексу України. За станом законодавства і постанов Пленуму Верховного Суду України на 1 грудня 2001 р./ За ред. С.С. Яценка. – К.: А.С.К., 2002. – С. 783-784.

[2] [115] Розенфельд Н. Відповідальність за незаконне втручання в роботу ЕОМ (комп’ютерів) // Вісник прокуратури. - 2002. - №4. - С. 23 – 27.

Комп’ютерна інформація. Описані вище специфічні характеристики інформації як предмета суспільного відношення, що виступає об’єктом незаконного втручання в роботу електронно-обчислювальних машин, систем та комп’ютерних мереж, дають можливість віднести цей склад до числа тих, у яких *предмет злочину* збігається з *предметом суспільного відношення*. Як правильно стверджує В.Я. Тацій, це "має місце, коли ті чи інші предмети, які входять до структури об’єкта злочину, законодавець наділяє додатково і функціями предмета суспільного відношення, тобто дає йому ще додатково й інше правове значення".[1] Саме така ситуація виявляється в складі незаконного втручання в роботу електронно-обчислювальних машин, систем та комп’ютерних мереж: саме з властивостями комп’ютерної інформації законодавець пов’язує наявність у діях особи складу злочину.

Об’єкт і предмет будь-якого злочину є взаємозалежними, взаємообумовленими. Тому, аналізуючи ознаки предмета незаконного втручання, необхідно виходити з викладеної у § 3 характеристики змісту безпосереднього об’єкта як *відносин власності на інформацію*.

Загальновизнаним в кримінальному праві є точка зору, що предмет злочину характеризується сукупністю трьох ознак: фізичної, економічної та юридичної. Тому, визначаючи інформацію предметом незаконного втручання, треба проаналізувати її ознаки.

Фізична ознака. Специфіка комп’ютерної інформації як предмета злочину полягає в неможливості її віднесення ні до матеріальних, ні до нематеріальних предметів. Як раніше було сказано, інформація як нематеріальний предмет включається в систему суспільних відносин за допомогою матеріального носія. Інакше кажучи, фізична ознака комп’ютерної інформації як предмета злочину полягає в її носії, що, зазвичай, розуміється як предмет, річ, властивості якої використовуються для

[1] [71] Кримінальне право України: Загальна частина: Підручник для студентів юрид. спец. вищ. закладів освіти /М. І. Бажанов, Ю.В. Баулін, В.І. Борисов та ін.; За ред. професорів М.І.

передачі, зберігання та опрацювання інформації. Носіями комп'ютерної інформації є дискети, оптичні та жорсткі диски і т.і. Визначаючи носій комп'ютерної інформації, необхідно враховувати, що однією з найважливіших характеристик сучасного етапу комп'ютеризації є розвиток електронних засобів зв'язку. Тому деякими дослідниками[1] ставиться питання про статус інформації, яка передається каналами зв'язку. Інформація в цих каналах передається за допомогою сигналів, які теж є матеріальними носіями передавання інформації.[2] Наприклад, електричні сигнали в телефонних лініях зв'язку можуть бути носіями інформації в комп'ютерних мережах. Саме таке розуміння носія комп'ютерної інформації дозволить визначати як знищення або пошкодження комп'ютерної інформації не тільки випадки впливу на пристрої комп'ютера, але й на сигнали, що передаються між комп'ютерами.

Таким чином, фізичною ознакою комп'ютерної інформації як предмета злочину є наявність носія – *предмета або сигнала, фізичні, хімічні чи інші властивості яких використовуються для зберігання, передавання та опрацювання інформації, що розпізнається електронно-обчислювальною машиною.*

У зв'язку з цим слід визнати, що виділення в диспозиції статті 361 КК як самостійного предмета злочину носія інформації є зайвим: носій самий по собі, без наповнення його інформацією, *інтересу не становить*. Лише виступаючи фізичною ознакою такого специфічного предмета злочину, як інформація, він включається до складу незаконного втручання і заподіяння йому шкоди цілком охоплюється поняттям знищення або перекручення комп'ютерної інформації. *Тому для вдосконалення диспозиції ст. 361 КК треба виключити вказівку на носій інформації.*

Бажанова, В.В. Сташиса, В.Я. Тація. – Київ-Харків: Юрінком Інтер-Право, 2001. – С. 95-96.

[1] Див., наприклад: [121] Семилетов С.И. Информация как особый нематериальный объект права //Государство и право. – 2000. – № 5. – С. 67-74.

[2] [149] Філософський словник / За ред. В.І. Шинкарука. – К.: Головна редакція УРЕ. 1973. - С. 471.

Інформація як предмет злочину має *економічну ознаку,* ціну, яка, урешті-решт, визначається її змістом і зацікавленістю споживача в її одержанні. Економісти відмічають, що як товар інформація має цілий ряд специфічних властивостей: "незнищуваність у процесі споживання; можливість багатократного споживання багатьма користувачами; у процесі передавання споживачу вона не втрачається для виробника; невизначеність і суб'єктивність корисності інформації; інформація характеризується достовірністю, надійністю та доступністю, але при цьому її доступність є різною для різних економічних аґентів; виробнику інформації заздалегідь споживач невідомий; неможлива однозначна вартісна оцінка виробленого обсягу інформації; особливий механізм її старіння – вона не зношується, а втрачає актуальність".[1] Цінність інформації буває різною: інформація може бути цінною *по суті*, оскільки є результатом тривалої роботи великої кількості осіб, а може бути цінною *за призначенням*, оскільки її наявність є необхідною умовою для вирішення певного завдання. При цьому цінність інформації як предмета злочину має одну особливість: її *корисні властивості* як фактор цінності не зводяться до фізичної цілісності її носія. Наприклад, комп'ютерна інформація може бути знищена або перекручена, а фізичні властивості носія залишаться незмінними. Виходячи із сказаного, до економічної ознаки комп'ютерної інформації слід віднести не тільки наявність ціни, але й наявність *корисних властивостей*, що дозволяють задовольняти інформаційну потребу. Ці властивості видається можливим описати так:

- цілісність – захищеність від несанкціонованих змін;
- доступність – захищеність від несанкціонованого блокування інформаційних ресурсів;

[1] [95] Новиков О.А., Мясникова Л.А. Логистика и коммерция информационного общества //Проблемы развития внешнеэкономических связей и привлечения иностранных инвестиций: региональный аспект: Сборник научных трудов. – Донецк, 1999. – С.118

- конфіденційність – захищеність від несанкціонованого одержання комп'ютерної інформації*.

З урахуванням викладеного, економічна ознака комп'ютерної інформації як предмета злочину виражається в тому, що вона *є цілісною, доступною, конфіденційною, і має ціну*.

Юридична ознака комп'ютерної інформації виражається в тому, що вона повинна бути *чужою* для винного та повинна мати свого власника.

Викладені ознаки комп'ютерної інформації як предмета злочину дозволяють критично оцінити позицію деяких авторів, які до комп'ютерної інформації відносять не тільки відомості, що людина зберігає, опрацьовує або передає за допомогою ЕОМ, але й комп'ютерні програми.[1] Таке положення є неправильним, оскільки поняття "інформація" пов'язане з такою категорією, як "код", тобто з *знанням* закономірності зміни стану об'єкта, що відображує, у залежності від змін об'єкта, що відображується. Питання про те, чи може "знати" електронно-обчислювальна машина, досить складне, тому що такого роду міркування приводять до проблеми штучного інтелекту. Зрозуміло, що на сучасному етапі розвитку комп'ютерної технології електронно-обчислювальні машини не виконують функції штучного інтелекту, а, отже, вести мову про інформацію у формі, яку "розуміє" машина, теж неправильно.

У цьому зв'язку заслуговує на увагу позиція В. Тюхтіна, котрий вважає інформацію властивістю суто людської свідомості та спілкування і пов'язує її

---

* Ця сукупність ознак одержала назву критеріїв безпеки інформаційної технології ITSEC (Information Technology Security Evaluation Criteria), які було прийнято в 1991 році співтовариством чотирьох європейських держав (Франції, Німеччини, Нідерландів і Великобританії). Зараз застосовуються для характеристики не тільки технічної захищеності системи, але й для характеристики ефективності правових механізмів охорони суспільних відносин з приводу комп'ютерної інформації.

[1] Див., наприклад: [142] Уголовный кодекс Украины: Научно-практический комментарий /Отв. ред. С.С. Яценко, В.И. Шакун). – К.: Правові джерела, 1998. – С. 815; [141] Уголовный кодекс Украины. Комментарий /Под ред. Ю.А. Кармазина и Е.Л. Стрельцова. – Х.: ООО "Одиссей", 2001. – С. 747.

з наявністю суб'єкта, який пізнає.[1] Це зауваження можна використати як методологічний принцип для розмежування способів порушення права власності на комп'ютерну інформацію. Так, комп'ютерна інформація може знищуватися, перекручуватися, блокуватися безпосередньо, а можна ті ж дії зробити шляхом зміни або знищення комп'ютерної програми, що використовується для роботи з нею.

Виходячи з викладеного, комп'ютерну інформацію як предмет злочину видається можливим визначити таким чином: **відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника і ціну.**

Комп'ютерна інформації як предмет злочину поділяється на два види: комп'ютерна інформація з обмеженим доступом та відкрита комп'ютерна інформація.

До інформації *з обмеженим доступом*, згідно зі статтею 30 Закону України "Про інформацію"[2], відноситься таємна і конфіденційна інформація.

До таємної інформації належать відомості, що становлять державну й іншу таємницю, передбачену законом, розголошення якої завдає шкоди особі, суспільству, державі.

Державна таємниця – вид таємної інформації, яка охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України та які віднесено законом до державної таємниці і поставлено під охорону з боку держави. Віднесення інформації до державної таємниці та порядок її використання визначаються Законом України "Про

---

[1] [79] Кузнецов Н.А., Мусхелишвили Н.Л., Шрейдер Ю.А. Информационное взаимодействие как объект научного исследования //Вопросы философии. – 1999. – № 2. – С. 78

[2] [52] Закон України "Про інформацію" від 2.11.1992 року //Закони України. Т. 4. – К., 1996. – С. 72-88.

державну таємницю" від 21 січня 1994 року.[1] Перелік відомостей, що становлять державну таємницю, затверджується наказом Голови Служби безпеки України.

Конфіденційна інформація – це відомості, які знаходяться у володінні, використанні або розпоряджанні окремих фізичних або юридичних осіб і розповсюджуються на їх розсуд та відповідно до передбачених ними умов. Виходячи з аналізу частини 3 статті 30 Закону України "Про інформацію"[2], можна залежно від характеру, змісту відомостей, що складають конфіденційну інформацію, виділити такі її види: професійна, ділова, виробнича, банківська, комерційна, іншого характеру. Громадяни та юридичні особи, котрі володіють інформацією професійного, ділового, комерційного та іншого характеру, придбаною на власні кошти, або такою, що є предметом їх професійного, ділового, комерційного та іншого інтересу, самостійно визначають її належність до конфіденційної. Наприклад, комерційною таємницею, відповідно до статті 30 Закону України "Про підприємства в Україні" від 22 березня 1991 року[3], є відомості, що пов’язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства і що не є державною таємницею, але розголошення яких може завдати шкоди інтересам підприємства.Перелік відомостей, що складають комерційну таємницю підприємства, порядок роботи з ними та організація їх охорони визначаються наказом керівника, зміст якого не повинен суперечити положенням чинного законодавства. Підставою для прийняття такого наказу служить частина 2 статті 30 Закону "Про підприємства в Україні"[4]: "Склад та обсяг відомостей, що складають

---

[1] [50] Закон України "Про державну таємницю" від 21.01.1994 року //Закони України. Т. 7. – К., 1997. – С. 38-50.

[2] [52] Закон України "Про інформацію" від 2.11.1992 року //Закони України. Т. 4. – К., 1996. – С. 72-88.

[3] [53] Закон України "Про підприємства в Україні" від 22.03.1991 року //Закони України. Т. 1. – К., 1995. – С. 310 -331.

[4] [53] Там само.

комерційну таємницю, порядок їх захисту визначаються керівником підприємства". Перелік відомостей, які не можуть складати комерційну таємницю, міститься в Постанові Кабінету Міністрів України № 611 від 9 серпня 1993 року "Про перелік відомостей, які не складають комерційну таємницю".

Відкриту комп'ютерну інформацію, виходячи з аналізу змісту статті 30 Закону України "Про інформацію"[1], можна визначити як таку, що не є інформацією з обмеженим доступом і може бути використана будь-якою особою.

Другим специфічним видом предмета незаконного втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж стаття 361 КК називає комп'ютерний вірус. Термін "комп'ютерний вірус" уперше застосував Фред Коен у 1984 році. Він пропонував таке визначення: "Комп'ютерний вірус – програма, яка може заражати інші програми, змінюючи їх шляхом доповнення своєї, можливо, зміненої, копії".[2] Пізніше з'явилися інші визначення комп'ютерного вірусу. Наприклад, на думку китайських спеціалістів, комп'ютерний вірус – це такий параметр, який проникає в комп'ютерну програму та порушує функціонування комп'ютера і здатний самостійно копіювати комп'ютерні команди або заміняти програмні дані.[3] А.М. Ришелюк визначає комп'ютерний вірус як комп'ютерну програму, здатну у випадку її активізації порушувати нормальну роботу автоматизованої електронно-обчислювальної машини, системи або комп'ютерної мережі, а також знищувати або пошкоджувати комп'ютерну інформацію.[4] Як вважає

---

[1] [52] Закон України "Про інформацію" від 2.11.1992 року //Закони України. Т. 4. – К., 1996. – С. 72 -88.

[2] Наводиться за: [59] Коваленко М.М. Комп'ютерні віруси і захист інформації. – К.: Наукова думка, 1999. – С. 7.

[3] [107] Положение по обеспечению безопасности компьютерных информационных систем в КНР //Борьба с преступностью за рубежом (по материалам зарубежной печати) //Ежемесячный информационный бюллетень. – М.: 1996 – № 9.

[4] [91] Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001 року /За ред. М.І. Мельника, М.І. Хавронюка. – К.: Каннон, 2001. – С. 904.

А.В. Загіка, комп'ютерний вірус являє собою "спеціальну програму або частину програми, здатну довільно приєднуватися до інших програм (тобто "заражати" їх) та при запуску останніх виконувати різні небажані дії: псування файлів, каталогів, перекручення результатів обчислень, знищення або перекручення інформації тощо".[1]

Слід зазначити, що, незважаючи на велику кількість різних підходів до визначення комп'ютерного вірусу, фахівці в цій галузі констатують, що на сьогодні чіткої його дефініції немає.[2] Проте аналіз наведених визначень дозволяє виділити дві основні ознаки комп'ютерних вірусів: по-перше, вони являють собою комп'ютерну програму, а, по-друге, ця програма призначена для знищення або перекручення комп'ютерної інформації. З цього випливає, що *комп'ютерний вірус за своєю суттю є одним із видів програмних засобів, призначених для незаконного проникнення в електронно-обчислювальні машини, системи або комп'ютерні мережі та здатних спричинити перекручення або знищення інформації.*

Викладене дозволяє зробити висновок, що виділення в диспозиції статті 361 КК України комп'ютерного вірусу як самостійного предмета злочину, який розповсюджується шляхом використання програмних і технічних засобів, призначених для незаконного проникнення в електронно-обчислювальні машини, системи або комп'ютерні мережі та здатних спричинити перекручення або знищення інформації, є некоректним і не відбиває його суті. Більш правильною була б така характеристика предмета аналізованого злочину: *програмні та технічні засоби, призначені для незаконного проникнення в електронно-обчислювальні машини, системи або комп'ютерні мережі та здатні спричинити перекручення або знищення інформації.* Саме таке розуміння буде повною мірою відбивати зміст

---

[1] [141] Уголовный кодекс Украины. Комментарий /Под ред. Ю.А. Кармазина и Е.Л. Стрельцова. – Х.: ООО "Одиссей", 2001. – С. 748.

[2] [59] Коваленко М.М. Комп'ютерні віруси і захист інформації. – К.: Наукова думка, 1999. – С. 7.

аналізованого предмета злочину, а отже, і відповідати його безпосередньому об’єкту.

У подальшому викладі програмні та технічні засоби, призначені для незаконного проникнення в електронно-обчислювальні машини, системи або комп’ютерні мережі та здатні спричинити перекручення або знищення інформації, будуть називатися *шкідливими програмними та технічними засобами*. Таке визначення видається обґрунтованим, оскільки сутність цих предметів полягає в тому, що вони призначені для заподіяння шкоди суспільним відносинам власності на комп’ютерну інформацію. Якщо визначення комп’ютерної інформації як предмета злочину пов’язане з її соціально корисними властивостями, то визначення як предмета злочину шкідливих програмних і технічних засобів відбиває їх *виняткові соціально шкідливі якості*. Характерною особливістю даної групи предметів комп’ютерного злочину є їх спеціальне призначення – знищення або перекручення інформації. На відміну від будь-яких інших комп’ютерних програм, шкідливі програмні та технічні засоби спеціально розробляються для незаконного втручання в роботу комп’ютерів, систем і комп’ютерних мереж. Саме це і визначає їхню специфіку.

Тому під *програмними засобами*, спеціально призначеними для незаконного втручання в роботу ЕОМ, систем і комп’ютерних мереж, слід розуміти програми (програмні блоки, програмне забезпечення), розроблені спеціально для її перекручення, знищення, незаконного копіювання, для несанкціонованого доступу до комп’ютерної інформації або для вчинення інших порушень права власності на неї.

Технічні засоби, спеціально призначені для порушення права власності на комп’ютерну інформацію, – це різного роду пристрої, устаткування,

розроблені для одержання незаконного доступу до комп'ютерної інформації, її знищення або перекручення.[1]

Таким чином, проведене дослідження предмета незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж дозволяє виділити такі види предметів цього злочину:

– комп'ютерна інформація – відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника і ціну;

– шкідливі програмні засоби – програми (програмні блоки, програмне забезпечення), розроблені спеціально для несанкціонованого доступу до комп'ютерної інформації, для перекручення, знищення, незаконного копіювання такої інформації або для вчинення інших порушень права власності на неї;

– шкідливі технічні засоби – різного роду пристрої, обладнання, спеціально розроблені для отримання незаконного доступу до комп'ютерної інформації, її знищення або перекручення, іншого порушення права власності на неї.

[1] [92] Науково-практичний коментар Кримінального кодексу України: за станом постанов Пленуму Верховного Суду України на 1 січня 1997 р. /За ред. В.Ф. Бойка, Ю.М. Кондратьєва, С.С. Яценка. – К.: Юрінком, 1997. – С. 723.

Розділ 2
ОБ'ЄКТИВНА СТОРОНА НЕЗАКОННОГО ВТРУЧАННЯ В РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН, СИСТЕМ І КОМП'ЮТЕРНИХ МЕРЕЖ

Аналіз об'єктивних ознак будь-якого конкретного складу злочину повинен грунтуватися на загальних положеннях, що стосуються характеристики загального поняття об'єктивної сторони. Тому й аналіз об'єктивної сторони незаконного втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж базується, насамперед, на загальних положеннях, які відносяться до об'єктивної сторони складу злочину, достатньо досліджені та арґументовані:

1) об'єктивна сторона складу злочину – це зовнішня сторона (зовнішнє вираження) злочину, яка характеризується суспільно небезпечним діянням (дією або бездіяльністю), суспільно небезпечними наслідками, причинним зв'язком, місцем, часом, обстановкою, способом, а також знаряддями й засобами скоєння злочину;

2) обов'язковою ознакою об'єктивної сторони будь-якого складу злочину є діяння (дія або бездіяльність), яке характеризується необхідною сукупністю чотирьох ознак (властивостей) – фізичної, соціальної, психологічної та юридичної;

3) залежно від законодавчої конструкції об'єктивної сторони складу злочину та її структури всі склади поділяються на формальні та матеріальні: для наявності об'єктивної сторони злочину з формальним складом достатньо встановити лише діяння (дію або бездіяльність), передбачене законом; віднесення законом суспільно небезпечного посягання до злочинів із матеріальним складом означає, що його об'єктивна сторона як обов'язкові

ознаки передбачає не тільки діяння, але й суспільно небезпечні наслідки та причинний зв'язок.[1]

Дослідження об'єктивної сторони незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж потребує ретельного аналізу диспозиції ст. 361 КК, оскільки, за загальним правилом, саме об'єктивна сторона найповніше описується законом і тим самим виконує найважливіші функції: визначає наявність злочину, його кваліфікацію, відмежування від суміжних. Як вдало відмічав М.І. Бажанов, "об'єктивна сторона злочину – це найважливіший елемент складу злочину, за яким у переважній більшості один злочин відрізняється від іншого. Тому законодавець прагне описати в диспозиції статті Особливої частини КК насамперед ознаки об'єктивної сторони".[2] Частина 1 ст. 361 КК описує об'єктивну сторону так: "Незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем та 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".

Диспозиція статті дозволяє зробити висновок про те, що об'єктивна сторона незаконного втручання може виражатися у двох формах, які мають свою специфіку в структурі та змісті:

1) незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем та комп'ютерних мереж, що призвело до

---

[1] Див.: [71] Кримінальне право України: Загальна частина: Підручник для студентів юрид. спец. вищ. закладів освіти /М.І. Бажанов, Ю.В. Баулін, В.І. Борисов та ін.; За ред. професорів М.І. Бажанова, В.В. Сташиса, В.Я. Тація. – Київ-Харків: Юрінком Інтер – Право, 2001. – С. 118

[2] [5] Бажанов М.И. Уголовное право Украины. Общая часть. – Днепропетровск: Пороги, 1992. – С. 341.

перекручення або знищення комп'ютерної інформації чи носіїв такої інформації;

2) розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані електронно-обчислювальні машини, їх системи або комп'ютерні мережі і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації;

Саме це вимагає самостійного аналізу даних форм.

2.1. Незаконне втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж, що спричинило перекручення або знищення комп'ютерної інформації

Ця форма об'єктивної сторони сконструйована як матеріальний склад злочину і, отже, потребує аналізу трьох ознак:

- діяння;
- наслідків;
- причинного зв'язку.

Діяння як ознака об'єктивної сторони аналізованого злочину в названій формі виражається в незаконному втручанні в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж. Тому, залежно від технічного засобу, втручання у його роботу може бути трьох видів:

- незаконне втручання в роботу електронно-обчислювальної машини;
- незаконне втручання в роботу електронно-обчислювальної системи;
- незаконне втручання в роботу комп'ютерної мережі.

Втручання* слід розуміти як *зміну режиму роботи* електронно-обчислювальної машини, системи або комп'ютерної мережі.

Специфіка *фізичної* ознаки втручання виявляється в тому, що: *втручання можливе тільки шляхом впливу на матеріальний носій інформації.* Це випливає з того, що наслідки у вигляді знищення або перекручення інформації, які є обов'язковою ознакою об'єктивної сторони даної форми аналізованого злочину, можна спричинити тільки шляхом впливу на носій. Така характеристика фізичної ознаки втручання свідчить про те, що воно може виражатися тільки в активній поведінці – *у дії.* У літературі з питання про поняття та зміст дії немає єдиної точки зору.

Відомо, що в основі дії лежить рух тіла. Однак деякі автори вважають, що дія обмежується тільки рухом тіла. Так, на думку В.М. Кудрявцева, людська дія обмежується усвідомленим рухом тіла, і тому є неправильним включати в поняття дії сили та закономірності, які використовує особа у своїй діяльності.[1] М.Д. Дурманов, навпаки, стверджував, що дія охоплює собою не тільки рух тіла людини, але й ті сили та закономірності, котрі вона використовує.[2] Автори "Курсу кримінального права" за редакцією Н.Ф. Кузнєцової та І.М. Тяжкової доходять компромісного висновку, що лише "доти, доки використовувані сили та закономірності є підконтрольними особі, можна говорити про злочинну дію в кримінально-правовому розумінні".[3] Видається, що остання точка зору є більш обґрунтованою і такою, яка відображує суть фізичної властивості діяння: в аналізованому складі дія є складною – це не просто рух тіла, це такий рух тіла, зміст якого з необхідністю включає процес використання певних

---

* У Тлумачному словникові С.І. Ожегова та Н.Ю. Шведової термін "втрутитися" подається так: "узяти участь у якій-небудь справі з метою зміни її ходу".

[1] [77] Кудрявцев В.Н. Объективная сторона преступления. – М.: Госюриздат, 1960. – С. 78.

[2] [48] Дурманов Н.Д. Понятие преступления. – М.- Л.: Издательство АН СССР, 1948. – С. 54.

[3] [83] Курс уголовного права. Общая часть. Том 1: Учение о преступлении: Учебник для вузов /Под ред. Н.Ф. Кузнецовой, И.М. Тяжковой. – М.: Зерцало, 1999. – С. 222.

складних закономірностей функціонування комп'ютерної техніки, що дозволяють заподіяти шкоду суспільним відносинам власності на інформацію. У зв'язку з цим *фізичну властивість* втручання можна визначити як *зміну режиму роботи ЕОМ, системи або комп'ютерної мережі шляхом впливу на носій (носії) комп'ютерної інформації.*

Саме це і дозволяє розкрити суспільну небезпечність діяння як його *соціальну* ознаку, а також визначити механізм заподіяння шкоди інформаційним відносинам у сфері використання комп'ютерної техніки. Незаконне втручання як суспільно небезпечне діяння ставить під погрозу функціонування електронно-обчислювальних машин, систем та комп'ютерних мереж у сфері зберігання, опрацювання, зміни, доповнення, передавання й одержання інформації.

Протиправність як обов'язкова ознака незаконного втручання полягає в тому, що це діяння є порушенням встановленого нормативно-правовими актами режиму роботи електронно-обчислювальних машин, систем або комп'ютерних мереж, відповідальність за яке, за умови настання певних наслідків, передбачено в кримінальному законі.

Специфіка *психологічної* ознаки незаконного втручання полягає в тому, що воно не просто є свідомою та вольовою поведінкою. Складність його фізичної властивості передбачає знання ознак предмета злочину, свідоме використання електронно-обчислювальних машин, систем та комп'ютерних мереж для завдання шкоди.

Викладене дозволяє дати таке визначення діяння як обов'язкової ознаки першої форми об'єктивної сторони складу злочину, передбаченого статтею 361 КК України: *втручання в роботу ЕОМ, систем або комп'ютерних мереж – зміна шляхом впливу на носій інформації режиму їх роботи, що порушує встановлений нормативно-правовими актами порядок використання ЕОМ.*

Як вже було підкреслено, за законодавчою конструкцією об’єктивної сторони незаконне втручання відноситься до числа так званих злочинів із матеріальним складом, тобто таких, обов’язковою ознакою яких, крім діяння, є певні, передбачені законом наслідки, тобто та шкода, що заподіюється злочинною діяльністю людини суспільним відносинам, які охороняються кримінальним законом.[1] Характеризуючи значення суспільно небезпечних наслідків, ще Чезаре Беккаріа правильно писав: "Істинним мірилом злочинів є шкода, яка завдається ними суспільству. Це одна з тих очевидних істин, для відкриття яких не потрібні ані квадранти, ані телескопи та які є доступними будь-якому середньому розуму".[2]

Безперечним є також і те, що якісні характеристики суспільно небезпечних наслідків залежать від змісту об’єкта посягання. На думку Н.Ф. Кузнєцової, злочинний наслідок – це об’єднуюча ланка між об’єктом і злочинним діянням.[3] А.О. Пінаєв прямо пише, що наслідки визначаються об’єктом злочину.[4]

Структура наслідку всебічно досліджена В.Н. Кудрявцевим, який вважає, що до його складу входять: а) порушення фактичного суспільного відношення, заради якого встановлено цю кримінально-правову норму; б) порушення відповідних правових відносин. У злочинах, які скоюються шляхом впливу на матеріальні предмети, наслідок включає в себе третій елемент – матеріальний.[5] Цю структуру можна застосувати і для визначення структури наслідків незаконного втручання в роботу електронно-обчислювальних машин, їх систем та комп’ютерних мереж. Елементами

---

[1] [89] Михлин А.С. Последствия преступления. – М.: Юридическая литература, 1969. – С. 16.

[2] [12] Беккариа Чезаре. О преступлениях и наказаниях. – М., 1939. – С. 226.

[3] [80] Кузнецова Н.Ф. Значение преступных последствий для уголовной ответственности. – М.: Государственное издательство юридической литературы, 1958. – С. 10.

[4] [102] Пинаев А.А. Уголовно-правовая борьба с хищениями. – Х.: Издательское объединение "Вища школа", 1975. – С. 58.

[5] [77] Кудрявцев В.Н. Объективная сторона преступления. – М.: Госюриздат, 1960. – С. 145-150.

наслідку в аналізованому складі є: 1) порушення суспільних відносин користування, володіння, розповсюдження комп'ютерної інформації з використанням ЕОМ, їх систем або комп'ютерних мереж; 2) порушення правовідносин власності на комп'ютерну інформацію; 3) знищення або перекручення інформації (матеріальний елемент). Диспозиція статті 361 КК України як наслідок незаконного втручання в роботу електронно-обчислювальних машин, систем або комп'ютерних мереж саме й передбачає знищення або перекручення комп'ютерної інформації – кінцевий результат названих порушень.

Щодо питання про поняття "знищення комп'ютерної інформації" у літературі немає єдиної думки. Деякі вчені вважають, що під знищенням інформації слід розуміти стирання її в пам'яті ЕОМ[1] або втрату інформації за умови неможливості її відновлення.[2] В.В. Крилов під знищенням комп'ютерної інформації розуміє повну фізичну ліквідацію інформації або ліквідацію таких її елементів, які впливають на зміну істотних ідентифікуючих, інформаційних ознак.[3] Такі визначення знищення комп'ютерної інформації є прийнятними для опису технічних характеристик наслідку і, безумовно, важливими для кримінального права. Водночас вони не розкривають кримінально-правового змісту поняття "знищення комп'ютерної інформації". Кримінально-правовий зміст цього поняття повинен відбивати насамперед ознаки, які характеризують соціально небезпечні властивості цього наслідку.

Видаються більш обґрунтованими визначення знищення комп'ютерної інформації як приведення інформації в цілому чи в істотній її частині в

---

[1] [63] Комментарий к Уголовному кодексу Российской Федерации. Издание 2-е, измененное и дополненное /Под общ. ред. Ю.И. Скуратова и В.М. Лебедева. – М.: Издательская группа Норма-Инфра М, 1998. – С. 415.

[2] [61] Комментарий к Уголовному кодексу Российской Федерации /Отв. ред. д-р юрид. наук, проф. А.В. Наумов. – М.: Юристъ, 1996. – С. 664

[3] [76] Крылов В.В. Информационные компьютерные преступления. – М.: Издательская группа Инфра М-Норма, 1997. – С. 47

непридатний для використання за призначенням стан[1] або припинення існування комп'ютерної інформації, приведення її в такий стан, коли її не можна відновити або використати за призначенням.[2] Однак і ці визначення є неповними, оскільки не відбивають такої ознаки наслідку, як протиправність, не дозволяють з'ясувати ті правові відносини, яким знищення інформації може завдати шкоди.

Певною мірою цей недолік усувається авторами Науково-практичного коментаря до КК України, які визначають знищення інформації як її втрату, коли інформація в АС перестає існувати для фізичних і юридичних осіб, що мають право власності на неї у повному чи обмеженому обсязі.[3] Водночас слід звернути увагу, що й таке визначення є не точним: воно дозволяє вважати знищенням інформації випадки, коли з технічної точки зору її не знищено, а, наприклад, переміщено на носій особи, яка не має права власності на таку інформацію, або вилучено носій комп'ютерної інформації чи блоковано інформацію .

Крім того, неповнота наведених визначень поняття знищення комп'ютерної інформації як обов'язкового наслідку незаконного втручання виявляється в тому, що вони не відбивають специфіки безпосереднього об'єкта цього злочину.

Видається, що повніше розкриватиме суть досліджуваного злочину таке визначення: *знищення комп'ютерної інформації – це такий вплив на носій комп'ютерної інформації, унаслідок якого вона перестає існувати у формі, що дозволяє її опрацювання за допомогою комп'ютерної техніки,*

---

[1] [49]Дьяконов С.В., Игнатьев А.А., Лунеев В.В., Никулин С.И. Уголовное право. – М.: Издательская группа Норма-Инфра М, 1999. – С. 288.

[2] [62] Комментарий к Уголовному кодексу Российской Федерации /Отв. редактор В.И. Радченко – М.: Вердикт, 1996. – С. 646

[3] [92] Науково-практичний коментар Кримінального кодексу України: за станом постанов Пленуму Верховного Суду України на 1 січня 1997 р. /За ред. В.Ф. Бойка, Ю.М. Кондратьєва, С.С. Яценка. – К.: Юрінком, 1997. – С. 722-723.

стає непридатною для задоволення інформаційної потреби особи, котра має право власності на таку інформацію.

Слід зазначити, що комп'ютерна інформація в певних випадках її знищення деякий час фактично не втрачається: змінюється лише перший символ в імені файлу, і тому він стає непридатним під час використання стандартних, традиційних програмних засобів. Фізичне місце на носії, яке відповідає такому файлу, вважається вільним, тому інформація фактично втрачається лише після того, коли на це місце буде записано нову інформацію. Тобто у власника певний час є можливість відновити знищену інформацію. Із цього питання правильним видається рішення, запропоноване О.Г. Волєводзом, який пише, що можливість користувача відновити комп'ютерну інформацію за допомогою апаратно-програмних засобів або отримати її від іншого користувача не звільняє винного від відповідальності.[1]

Перекручення комп'ютерної інформації можна визначити за аналогією з пошкодженням майна: етимологічне значення терміна "перекручення" є близьким до значення терміна "пошкодження". Цей термін одержав досить повне визначення при аналізі злочинів проти власності. Пошкодження визначають як "погіршення якості, зменшення цінності речі або приведення речі на певний час у непридатний, за цільовим призначенням, стан"[2], або як "псування ... майна, у результаті якого воно втрачає свої якості настільки, що тимчасово або частково стає непридатним для використання його за

[1] [24] Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО Изд-во "Юрлитинформ", 2002. – С. 67 – 68.

[2] [112] Постанова Пленуму Верховного Суду України № 4 від 2 липня 1976 "Про питання, що виникли в судовій практиці в справах про знищення та пошкодження державного і колективного майна шляхом підпалу або внаслідок порушення правил пожежної безпеки" //Бюлетень законодавства і юридичної практики України. – 1995. – № 1. – С. 191.

призначенням, але після затрати праці та засобів на відновлення його колишньої якості це майно може бути використане за призначенням".[1]

У своїй основі ці визначення можна застосувати і до дефініції перекручення комп'ютерної інформації. Необхідно лише врахувати специфіку комп'ютерних технологій та інформаційних відносин. Виходячи з цієї специфіки, а також з урахуванням об'єкта досліджуваного складу перекручення комп'ютерної інформації можна визначити як *такий вплив на носій комп'ютерної інформації, який полягає в зміні без відома власника змісту відомостей, відбитих на носії, що робить інформацію повністю, частково або тимчасово непридатною для задоволення інформаційної потреби особою, яка має право власності на таку інформацію.*

Оскільки склад незаконного втручання відноситься до матеріальних, обов'язковою ознакою його об'єктивної сторони є наявність причинного зв'язку між діянням (незаконним втручанням у роботу електронно-обчислювальних машин) і наслідками у вигляді знищення або перекручення комп'ютерної інформації.

Розгляд цієї проблеми потребує, як видається, короткого аналізу найбільш відомих теорій причинного зв'язку, що мали місце в історії кримінального права. Такий аналіз дасть змогу встановити генезис наукових поглядів щодо причинного зв'язку, його змісту й одержати комплексне уявлення про цю проблему. Першою, досить поширеною, теорією причинного зв'язку була теорія еквівалентності. Вона визнавала причинний зв'язок між дією людини та злочинним наслідком, який настав, у всіх тих випадках, коли ця дія була необхідною попередньою умовою результату. Для встановлення того, що умова була необхідною, застосовувався метод уявного винятку, при чому прихильники цієї теорії всі попередні умови вважали рівноцінними. У цьому полягає основний недолік даної точки зору.

[1] [124] Сирота С.И. Преступления против социалистической собственности и борьба с ними. – Воронеж: Издательство Воронежского университета, 1968. – С. 156.

Критикуючи її, Т.В. Церетелі відзначала, що логічним наслідком такого підходу є поява різних суб'єктивних поглядів на поняття замаху, співучасті та самого злочину, у результаті чого кримінальне законодавство можна звести до однієї норми: "… всяка суспільно небезпечна людина повинна бути знешкоджена".[1]

Подальший розвиток вчення про причинний зв'язок був обумовлений вирішенням проблеми звуження меж умов, встановлених теорією еквівалентності. Так, К. Бікмайєром пропонувалася теорія нерівноцінності умов. На його думку, умови слід поділяти на "найбільш діючі" і "менш діючі". Однак чіткого методу їх визначення він не запропонував, вважаючи, що в цих питаннях треба керуватися здоровим глуздом. Тією чи іншою мірою ця теорія одержала відображення в роботах М.С. Таганцева і С.В. Познишева, але й вони чітких критеріїв обмеження кола попередніх умов також не висунули.[2]

Найбільш вдалим рішенням проблеми причинного зв'язку є теорія необхідного спричинення. Уперше вона була запропонована А.А. Піонтковським. В основі цієї теорії лежать філософські категорії випадкового та необхідного: кримінальна відповідальність ні за яких умов не повинна бути пов'язана з випадковими наслідками людської поведінки. Необхідний наслідок визначається А.А. Піонтковським як "прояв закономірності розвитку цього явища, воно внутрішньо йому властиве".[3] Описуючи необхідний причинний зв'язок, Г.А. Кригер відзначав, що "всяка причина – необхідна умова наслідків, але не навпаки: не всяка умова переростає в причину наслідків". Дуже вдалим був його висновок про те, що в кримінальному праві причинний зв'язок має місце лише тоді, "коли

---

[1] [153] Церетели Т.В. Причинная связь в уголовном праве. – М.: Государственное издательство юридической литературы, 1963. – С. 92.
[2] [150] Флетчер Дж., Наумов А.В. Основные концепции современного уголовного права. – М: Юристъ, 1998. – С.179-182.
[3] [150] Там само.

шкідливі наслідки, що настали, були закономірним наслідком такого діяння, у вчиненні якого, об'єктивних умовах і обставинах його вчинення, були закладені реальні можливості настання саме цих наслідків і настали вони без втручання третіх осіб або дії яких-небудь інших зовнішніх сил".[1]

Ця теорія причинного зв'язку є найбільш визнаною і саме вона щонайкраще дозволяє проаналізувати зміст причинного зв'язку в об'єктивній стороні незаконного втручання в роботу електронно-обчислювальних машин. У методологічному плані необхідність наслідку, згідно з теорією необхідного спричинення, визначається, виходячи з двох таких положень:

1) суспільно небезпечне діяння завжди передує настанню суспільно-небезпечних наслідків;

2) діяння за своїм характером внутрішньо (закономірно) містить у собі реальну можливість саме такого наслідку.

Ураховуючи викладене, можна дійти висновку: причинний зв'язок як обов'язкова ознака об'єктивної сторони аналізованої форми незаконного втручання в роботу електронно-обчислювальних машин полягає в тому, що незаконне втручання з необхідністю спричиняє знищення або перекручення комп'ютерної інформації, воно передує настанню зазначених суспільно небезпечних наслідків, містить у собі реальну можливість знищення або перекручення комп'ютерної інформації та в конкретному випадку є необхідною умовою, без якої наслідки у вигляді знищення або перекручення інформації не настали б.

Незаконне втручання в аналізованій формі буде закінченим із моменту настання суспільно небезпечних наслідків у вигляді знищення або перекручення інформації.

---

[1] [69] Кригер Г.А. Советское уголовное право. Общая часть: Учебник. – Изд. МГУ, 1988. – С. 116.

Значний інтерес при аналізі об’єктивної сторони незаконного втручання в першій формі становить питання про способи вчинення злочину. Незаконне втручання в цій формі характеризується різноманітністю способів, які можуть бути застосовані винними і залежать, як правило, від властивості та призначення комп’ютерної інформації, що знищується або перекручується. Як відомо, спосіб вчинення злочину – це "певний порядок, метод, послідовність рухів і прийомів, застосовуваних особою в процесі здійснення суспільно-небезпечного посягання на охоронювані кримінальним законом суспільні відносини, поєднаний із виборочим використанням засобів вчинення злочину".[1]

У загальному понятті складу злочину спосіб відноситься до факультативних ознак об’єктивної сторони, а, отже, у різних складах злочину, залежно від оцінки його законодавцем, може відігравати три різні ролі: обов’язкової ознаки, кваліфікуючої ознаки або ознаки, що обтяжує покарання. У даному складі спосіб *не є обов’язковою ознакою*, а тому не впливає на його кваліфікацію, однак його характеристика має велике значення для з’ясування характеру діяння, його суспільної небезпечності, а також для призначення покарання. У зв’язку з цим характеристика можливих способів незаконного втручання видається необхідною.

Різні способи незаконного втручання в роботу ЕОМ, систем і комп’ютерних мереж можна класифікувати на три групи, виходячи з такого критерію, як характер засобів, застосовуваних для вчинення незаконного втручання:

– способи, засновані на використанні засобів спеціального технічного впливу;

– способи, засновані на використанні програмного забезпечення;

– змішані способи.

---

[1] [100] Панов Н.И. Способ совершения преступления и уголовная ответственность. – Х.: Вища школа, 1982. – С. 44.

Способи першої групи зумовлені тим, що комп'ютерні технології, як і будь-який інший прилад або пристрій, не є абсолютно надійними. Під час роботи з ними значною є можливість їх відмови (такого стану, коли комп'ютер перестає бути придатним для використання) або збою (коли комп'ютер тимчасово не може використовуватися). Зрозуміло, що в разі відмови або збою комп'ютерної системи власник інформації не може здійснювати свої повноваження. Крім того, внаслідок відмови або збою комп'ютерна інформація може бути знищена, перекручена, блокована тощо. За Державним стандартом України 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни і визначення" для опису такого роду дій застосовується термін "спеціальний вплив", що визначається так: "вплив на технічні засоби, який приводить до здійснення загрози для інформації".[1] Вчинення незаконного втручання таким способом як правило пов'язано з використанням спеціальних приладів. Наприклад, існують заряди електромагнітної дії. Після їх вибуху на достатньо великому радіусі припиняють роботу комп'ютери та засоби зв'язку.[2]

Даний спосіб вчинення цього злочину пов'язаний із *фізичним впливом* на комп'ютерну техніку, носії інформації, що спричиняє порушення права власності на комп'ютерну інформацію. У результаті такого впливу порушується фізична цілісність комп'ютерної техніки, і тут може виникати питання про кваліфікацію таких дій як злочинів проти власності. Тому слід мати на увазі, що відмежовувати комп'ютерний злочин від злочину проти власності в таких випадках треба, виходячи з оцінки ознак суб'єктивної сторони: коли метою злочинця є пошкодження або знищення майна (комп'ютерної техніки), то має місце злочин проти власності; у випадку ж, коли дії злочинця спрямовані на заподіяння шкоди відносинам власності на

---

[1] [46] ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. – 1998. – 1 січня. – С. 5.

[2] [56] Кабанников А. Электронная "Хиросима" уже затаилась в Москве // Комсомольская правда. – 1998. – 16 декабря. – С. 5.

комп'ютерну інформацію, то має місце незаконне втручання в роботу електронно-обчислювальної машини, системи або комп'ютерної мережі.

Друга група способів вчинення досліджуваного злочину заснована на використанні програмного забезпечення, інтерфейсу користувача – комплексу програмних засобів, які забезпечують взаємодію користувача із системою.[1] Використовуючи наявне програмне забезпечення, злочинець здійснює описані вище дії у відношенні комп'ютерної інформації. Специфічною рисою цих способів є те, що комп'ютер продовжує функціонувати, але інформація, яка опрацьовується в ньому, знищується, спотворюється, копіюється тощо.

Третя група – змішані способи – заснована на використанні інтерфейсу для заподіяння шкоди фізичній цілісності комп'ютерної техніки, а отже, заподіяння шкоди відносинам власності на комп'ютерну інформацію. Наприклад, існує певна група шкідливих комп'ютерних програм, принцип роботи яких полягає в тому, що шляхом подання по черзі команд зчитування й запису інформації на жорсткому диску механізми жорсткого диска приводяться в резонансну частоту та руйнуються, а в результаті знищується інформація, яка зберігалася на цьому диску.

Можна назвати ще велику кількість способів незаконного втручання, але всі вони можуть бути віднесені до однієї з перерахованих вище груп. Деяку специфіку має лише один спосіб, який можна назвати *несанкціонованим доступом*. В українському кримінальному законодавстві та практиці його застосування такий спосіб не вказується. Однак, якщо звернутися до зарубіжного законодавства, то в ряді країн несанкціонований доступ передбачається як самостійний склад злочину.[2]

---

[1] [101] Першиков В.И., Савинков В.М. Толковый словарь по информатике. – Москва: Финансы и статистика, 1991. – С. 128.

[2] Для аналізу зарубіжного законодавства використано роботу [165] Stein Schjolberg, Chief Judge Moss byrett, Norway "The Legal Framework – Unauthorized Access to Computer Systems. Penal Legislation in 37 Countries", http://www.mossbyrett.of.no/legal.html.

Так, в Австралії стаття 76В частини VI А "Злочини, пов'язані з комп'ютерами" Закону про злочини Зводу законів Співдружності передбачає відповідальність за несанкціонований доступ. У цій статті вказуються такі ознаки несанкціонованого доступу, як відсутність в особи відповідних повноважень щодо роботи з комп'ютерною інформацією; інформація, до якої здійснюється доступ, знаходиться в комп'ютері, який належить державі (для опису такого комп'ютера застосовується термін "комп'ютер Співдружності").

У КК Німеччини*, Італії* та Нідерландів* також передбачено відповідальність за несанкціонований доступ. Однак у цих країнах до його обов'язкових ознак законодавець відносить наявність засобів захисту комп'ютерної інформації від несанкціонованого доступу.

Швейцарський законодавець для опису несанкціонованого доступу об'єднує ознаки об'єктивної та суб'єктивної сторін. Відповідно до статті 143bis "Незаконний доступ до систем опрацювання даних" Кримінального кодексу цієї держави таким вважається одержання доступу до *спеціально охоронюваної* інформації без мети отримання незаконної вигоди.

Певний інтерес викликає вирішення проблеми несанкціонованого доступу до комп'ютерної інформації, запропоноване білоруським законодавцем. Аналіз ст. 349 КК Республіки Білорусь "Несанкціонований доступ до комп'ютерної інформації" дозволяє дійти висновку, що таким буде доступ, який супроводжується порушенням систем захисту комп'ютерної інформації.[1]

---

* Стаття 202a Кримінального кодексу Німеччини.
* Стаття 615b Кримінального кодексу Італії.
* Стаття 138a Кримінального кодексу Нідерландів.
[1] [140]Уголовный кодекс Республики Беларусь / Вступ. Ст. А.И. Лукашова, Э.А. Саркисовой. – 2-е изд., испр. и доп. – Мн.: Тесей, 2001. – С. 218.

Незважаючи на відмінності в самих визначеннях, у більшості норм, які передбачають відповідальність за несанкціонований доступ, виділяється ознака, що відбиває не тільки правову специфіку, але й підвищену суспільну небезпечність цього способу. Такою ознакою *є наявність спеціальних засобів захисту комп'ютерної інформації, до якої здійснюється доступ*. Видається, що це дійсно розкриває особливість прийомів і методів, характерних для несанкціонованого доступу і таких, що визначають його підвищену суспільну небезпечність.

З урахуванням указаного вище несанкціонований доступ можна було б визначити так: *спосіб вчинення незаконного втручання в роботу ЕОМ, систем, комп'ютерних мереж, який полягає в одержанні винним можливості здійснювати різні дії з комп'ютерною інформацією, що має специфічні технічні або програмні засоби захисту від її знищення або перекручення.*

Захист комп'ютерної інформації забезпечується різними засобами:

- організаційними;
- технічними;
- програмними.

Організаційні засоби інформаційної безпеки полягають у відповідній роботі з персоналом, який працює з електронно-обчислювальнимим машинами, системами чи комп'ютерними мережами (добір, постійна перевірка, інструктажі), забезпеченні режиму таємності при функціонуванні комп'ютерних систем і фізичній охороні об'єктів, де опрацьовується, зберігається чи передається комп'ютерна інформація.[1]

До технічних засобів захисту комп'ютерної інформації відносяться різноманітні пристрої, які спеціально призначені для забезпечення цілісності, конфіденційності та доступності комп'ютерної інформації:

[1] [114] Расследование неправомерного доступа к компьютерной информации / Под. ред. Н.Г. Шуруханова. – М.: Щит – М, 1999. – С. 38 – 40.

джерела безперервного живлення апаратури, а також пристрої стабілізації напруги, мережні фільтри; засоби екранування апаратури, ліній проводового зв'язку та приміщень, у яких знаходиться комп'ютерна техніка; пристрої визначення та фіксації номера абонента, який отримує доступ до електронно-обчислювальної машини, системи чи комп'ютерної мережі, та інші пристрої, що забезпечують безпеку функціонування комп'ютерної техніки.[1]

Програмні засоби захисту комп'ютерної інформації являють собою комп'ютерні програми, які розроблені та використовуються спеціально для забезпечення безпеки процесів зберігання, передавання та опрацювання комп'ютерної інформації в електронно-обчислювальній машині, системі чи комп'ютерній мережі. Ці засоби видається можливим класифікувати за об'єктом захисту на три види:

- засоби, що забезпечують аутентифікацію користувача;
- засоби, що забезпечують безпеку комунікаційних ліній;
- засоби, що забезпечують цілісність інформаційних ресурсів.

Найбільш поширеною формою програмних засобів *аутентифікації користувачів* є встановлення різноманітних паролів доступу (access passwords): для входу в систему, зміни, доповнення чи знищення комп'ютерної інформації, для використання переферійного обладнання і т. ін.

Захист інформації, що передається (*безпека комунікаційних ліній*), зазвичай досягається шляхом шифрування даних перед їх введенням у канал зв'язку чи на фізичний носій. З цією метою використовуються комп'ютерні програми, у яких реалізовано криптографічні алгоритми. До таких програм, наприклад, відноситься загальновідома Diskreet з програмного пакета Norton Utilites.

[1] [114] Там само. – С. 40 – 41.

Проблема забезпечення *безпеки інформаційних ресурсів* найчастіше постає під час використання комп'ютерних мереж. Комплекс засобів, призначених для захисту інформаційних ресурсів, що розташовані в комп'ютерних мережах (мережних інформаційних ресурсів), має назву "брандмауер". Як інженерний термін "брандмауер" визначає стіну, за яку ні в якому разі не може поширитися вогонь, тому ці конструкції використовуються для захисту найцінніших об'єктів, що знаходяться в будинку. В інформаційних технологіях брандмауер використовується для захисту найціннішої інформації. Зазвичай брандмауери являють собою пакетні фільтри, які забезпечують доступ тільки санкціонованих користувачів до ресурсів мережі.[1] Однак для захисту інформаційних ресурсів використовуються не тільки такі комплекси. Більш простим, а тому більш поширеним засобом є архівація інформаційних ресурсів або їх архівація з використанням методів шифрування.[2]

Отже, несанкціонованим буде доступ до комп'ютерної інформації, яка охороняється технічними або програмними засобами захисту. Одним з видів незаконного втручання, поєднаного з порушенням технічних засобів захисту інформації, є електромагнітне перехоплення. Сучасні технології дозволяють отримувати інформацію в умовах відсутності безпосереднього підключення до комп'ютерної системи. Це досягається за рахунок перехоплення випромінювань центрального процесора, дисплея, комунікаційних каналів, принтера і т.д. Використання спеціального обладнання дозволяє "знімати" інформацію з комп'ютера, який знаходиться на достатньо великій відстані (у іншому приміщенні або будинку). У спеціальній літературі містяться відомості про те, що сучасні технічні засоби

[1] [17] Вакка Дж. Секреты безопасности в Internet. – К.: Диалектика, 1997. – С. 129.

[2] [154] Иванов В.Г., Коровин А.С. Алгоритм защиты и сжатия файлов // Правові основи захисту комп'ютерної інформації від протиправних посягань. Матеріали міжвузівської науково-практичної конференції (22 грудня 2000 року). - Донецьк: Донецький інститут внутрішніх справ, 2001. – С. 212 –215.

дозволяють знімати та розшифровувати випромінювання принтера, який працює на відстані до 150 метрів, випромінювання моніторів і кабелів зв'язку – до 500 метрів.[1] Виходячи з запропонованого визначення несанкціонованого доступу, використання такого обладнання для незаконного втручання в роботу електронно-обчислювальних машин, систем чи комп'ютерних мереж буде несанкціонованим доступом до комп'ютерної інформації лише у випадках, коли власник інформації застосовує будь-які спеціальні технічні чи програмні засоби її захисту. У разі коли комп'ютерна інформація не охороняється спеціальними засобами втручання, незаконне втручання шляхом електромагнітного перехоплення не містить ознак несанкціонованого доступу.

Відповідно до наведеної класифікації програмних засобів захисту комп'ютерної інформації видається можливим навести приклади несанкціонованого доступу, що полягає в подоланні таких засобів. Порушення програмних засобів аутентифікації користувача може полягати в доборі паролів. Наприклад, найбільш поширеним методом аутентифікації користувачів є протокол PAP (Password Authentification Protocol – протокол аутентифікації паролів), його робота полягає в тому, що ім'я користувача та його пароль передаються на сервер, де порівнюються з інформацією, яка знаходиться в базі даних. Для подолання такого захисту, як правило, здійснюється перехоплення пароля під час його передачі на сервер законним користувачем, після чого злочинець отримує доступ до системи від імені законного користувача та використовуючи його пароль.

Порушення програмних засобів, що забезпечують безпеку комунікаційних ліній, зазвичай виражається в роботі спеціальних програм дешифрування. Злочинець спостерігає потік інформації та за допомогою

[1] [114] Расследование неправомерного доступа к компьютерной информации / Под. ред. Н.Г. Шуруханова. – М.: Щит – М, 1999. – С. 106.

таких програм намагається встановити криптографічний алгоритм та розкрити ключ.

Найскладнішим засобам захисту комп'ютерної інформації – брандмауерам – відповідає найскладніший вид несанкціонованого доступу. Такий доступ часто називають "електронний злом". Найчастіше він здійснюється з декількох робочих місць (один неправомірний користувач легко виявляється). У заданий час декілька (більше десяти) неправомірних користувачів одночасно намагаються здійснити несанкціонований доступ. За такої кількості "атакуючих" комп'ютерів навіть найнадійніші системи захисту комп'ютерної інформації не встигають адекватно реагувати на створену нештатну ситуацію. Це призводить до того, що декілька неправомірних користувачів відсікаються системою захисту, а решта отримує доступ. Потім один з неправомірних користувачів блокує систему статистики, що фіксує всі спроби доступу, це дозволяє іншим неправомірним користувачам бути невиявленими та незафіксованими. Частина з них після цього починає "злом" потрібного інформаційного ресурсу, а решта займається фіктивними операціями з метою приховування злочину та дезорганізації роботи підприємства, установи чи організації, якій належить відповідний інформаційний ресурс.[1]

Необхідно також відзначити, що несанкціонований доступ має місце не тільки коли злочинець безпосередньо долає певний технічний чи програмний засіб захисту комп'ютерної інформації. Діяння матиме ознаки несанкціонованого доступу й у випадку, коли власник інформації використовує певну систему захисту, але злочинець отримує доступ до комп'ютерної інформації, не долаючи засоби захисту, а обходячи їх. Наприклад, до каналів витоку комп'ютерної інформації відносяться електричні канали, типовим середовищем для яких є стандартна

[1] [123] Сергеев В.В. Компьютерные преступления в банковской сфере // Банковское дело. - 1997. - № 2. - С 27. – 28.

електромережа.[1] Під час роботи електронно-обчислювальні машини створюють наводки в електричній мережі, аналіз яких дозволяє здійснити несанкціонований доступ до комп'ютерної інформації. Припустимо, що власник комп'ютерної інформації встановив засоби екранування обладнання (технічний засіб захисту комп'ютерної інформації) та систему аутентифікації користувачів (програмний засіб), але злочинець, не порушуючи ці засоби, отримує несанкціонований доступ через електричні канали витоку комп'ютерної інформації. У діях такої особи присутні ознаки несанкціонованого доступу до комп'ютерної інформації.

Слід зауважити, що подолання організаційних засобів захисту комп'ютерної інформації, наприклад проникнення в охоронюване приміщення, де розташовані електронно-обчислювальні машини, системи чи комп'ютерні мережі, не відноситься до несанкціонованого доступу. Це випливає з того, що такий спосіб вчинення незаконного втручання не підвищує його суспільної небезпечності. Водночас вчинення незаконного втручання шляхом порушення саме технічних чи програмних засобів захисту комп'ютерної інформації відбиває зміст несанкціонованого доступу як *найбільш небезпечного способу* незаконного втручання:

1) для подолання заходів інформаційної безпеки технічного або програмного характеру необхідні спеціальні знання, специфічні навики;
2) шкода власникові завдається не тільки у вигляді знищення або перекручення комп'ютерної інформації, але й у вигляді істотних матеріальних збитків, обумовлених необхідністю відновлення або заміни системи захисту (за даними фахівців з інформаційної

[1] [85] Логвиненко Н.Ф.,Емельянов С.Л., Носов В.В., Писаревский В.И. Современные методы и средства защиты компьютерной информации от утечки по электрическим каналам // Правові основи захисту комп'ютерної інформації від протиправних посягань. Матеріали міжвузівської науково-практичної конференції (22 грудня 2000 року). - Донецьк: Донецький інститут внутрішніх справ, 2001. – С. 190 –199.

безпеки, створення системи безпеки комп'ютерної інформації для крупної фінансової установи коштує близько 15 мільйонів доларів США[1]).

Саме це дозволяє обґрунтувати необхідність виділення несанкціонованого доступу як кваліфікуючої ознаки складу незаконного втручання. У зв'язку з цим ч. 2 ст. 361 КК України видається доцільним доповнити вказівкою на цю ознаку: "Ті самі дії … вчинені шляхом несанкціонованого доступу до комп'ютерної інформації".

2.2. Розповсюдження шкідливих програмних і технічних засобів

Друга форма об'єктивної сторони незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж сконструйована в законі як злочин із формальним складом і вважається закінченою з моменту вчинення самої дії – розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані електронно-обчислювальні машини, їх системи або комп'ютерні мережі і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації.

Виходячи з диспозиції ст. 361 КК, кримінально-караним є тільки таке розповсюдження комп'ютерного вірусу, яке здійснюється з використанням шкідливих програмних або технічних засобів. Як приклад таких дій можна змоделювати ситуацію: особа за допомогою програмного або технічного засобу "зламує" систему захисту комп'ютерної мережі та запускає в неї вірус. Водночас не можна не звернути уваги на те, що наведене в законі визначення є некоректним з точки зору сутності поняття "розповсюдження

[1] [114] Расследование неправомерного доступа к компьютерной информации / Под. Ред. Н.Г. Шуруханова. – М.: Издательство "Щит – М", 1999. – С. 44.

комп’ютерного вірусу". За особливостями розповсюдження комп’ютерні віруси поділяються на файлові, бутові (завантажувальні) та мережні. До файлових вірусів відносяться такі, що розповсюджуються шляхом упровадження в командні, виконавчі файли або файли драйверів, які завантажуються, тобто програм, до яких звертається і з якими працює користувач. Бутові віруси, або віруси, що завантажуються, розповсюджуються шляхом "зараження" завантажувального сектора гнучкого або жорсткого носія. Мережні віруси використовують для свого розмноження можливості спеціального програмного забезпечення, яке організовує функціонування комп’ютерної мережі. Наслідки використання таких вірусів, як правило, полягають у переповненні пам’яті комп’ютера, підключеного до мережі, копіями вірусу, що призводить до неможливості роботи з інформацією, яка міститься в цій ЕОМ.

Отже, розповсюдження комп’ютерного вірусу можна здійснити трьома способами:

– упровадженням вірусу в програми;

– "зараженням" завантажувального сектора носія;

– розповсюдженням вірусу з використанням мережного програмного забезпечення.[1]

Якщо виходити з буквального розуміння законом розповсюдження комп’ютерного вірусу зазначеним у статті 361 КК України способом, то можна зробити висновок, що диспозиція статті не повною мірою охоплює всі можливі способи розповсюдження комп’ютерного вірусу, які відомі в інформатиці та зустрічаються в практиці. Так, наприклад, наприкінці грудня 1987 року студент університету Clausthal-Zellerfeld (Німеччина) розробив вірус Christmas Tree (Різдвяна ялинка). Цей вірус належав до категорії мережних, і наслідки його роботи полягали в блокуванні комп’ютерів,

[1] [59] Коваленко М.М. Комп’ютерні віруси і захист інформації. – К.: Наукова думка, 1999. – С. 138-143.

підключених до мережі. Згідно з програмою його автора вірус розповсюджувався шляхом використання звичайного механізму електронної пошти.[1] Подібні суспільно небезпечні дії, якби вони були здійснені в Україні, не можна було б кваліфікувати за статтею 361 КК. Дії автора цього вірусу не підпадають під ознаки розповсюдження вірусу, передбаченого статтею 361 КК України, оскільки програмне забезпечення функціонування електронної пошти не є програмним засобом, призначеним для незаконного проникнення в роботу автоматизованих систем, тобто в даному випадку комп'ютерний вірус не розповсюджувався за допомогою шкідливого програмного або технічного засобу.

Крім того, як зазначалося раніше при аналізі предмета незаконного втручання, комп'ютерний вірус сам по собі і є шкідливим програмним засобом.

Сказане дозволяє зробити висновок про необхідність уточнення диспозиції статті 361 КК у тій частині, де вона характеризує цю форму об'єктивної сторони незаконного втручання. Видається, що більш вдалим було б таке її визначення: *розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в ЕОМ, системи або комп'ютерні мережі та здатних заподіяти перекручення або знищення комп'ютерної інформації*[*].

Таке формулювання дало б змогу:

1) більш точно визначити предмет цього злочину, позначивши його як будь-які шкідливі програмні та технічні засоби, а не тільки комп'ютерні віруси;

---

[1] [59] Там само. – С. 176.

[*] Цікаво відзначити, що саме таку пропозицію було внесено до Проекту КК кафедрою кримінального права Національної юридичної академії ім. Я. Мудрого в 1997 році, але, на жаль, її не було сприйнято законодавцем.

2) удосконалити характеристику об'єктивної сторони цього злочину з точки зору способу й засобів розповсюдження комп'ютерних вірусів;

3) забезпечити більш ефективний захист інформаційних відносин і правильну кваліфікацію вчинених дій.

З урахуванням таких змін об'єктивна сторона в цій формі незаконного втручання полягала б у таких видах діяння: 1) розповсюдженні *програмних засобів*, призначених для незаконного проникнення в ЕОМ, системи або комп'ютерні мережі та здатних спричинити перекручення або знищення комп'ютерної інформації; 2) розповсюдженні *технічних засобів*, призначених для незаконного проникнення в ЕОМ, системи або комп'ютерні мережі та здатних спричинити перекручення або знищення комп'ютерної інформації.

Важливо відмітити, що в літературі немає єдиного тлумачення самого поняття "розповсюдження шкідливих програмних і технічних засобів". Так, деякі вчені вважають, що розповсюдження програми для ЕОМ – це "надання доступу до відновленої у будь-якій матеріальній формі програми для ЕОМ, у тому числі мережними та іншими способами, а також шляхом продажу, прокату, здавання в найми, надання в позику, а рівно створення умов для саморозповсюдження програми".[1] Інші визначають це поняття як "… надання доступу до відновленої в будь-якій формі програми для ЕОМ, у тому числі мережним та іншими способами, а також шляхом продажу, здавання в найми, надання в позику, включаючи імпорт для будь-якої із зазначених цілей".[2] На думку третіх це "… будь-яка форма … реалізації – як на комерційній, так і на іншій основі, як із позначенням сутності програми, так і без нього, шляхом дублювання чи реалізації окремих машинних носіїв

[1] [137] Уголовное право России: Учебник для вузов в 2-х томах. Т. 2. Особенная часть /Под. ред. А.Н. Игнатьева, Ю.А. Красикова. – М.: Изд. группа Норма–Инфра М, 1998. – С. 601.
[2] [117] Российское уголовное право. Особенная часть: Учебник /Под. ред. М.П. Журавлева, С.И. Никулина М.: Спарк, 1998. – С. 339.

(флоппі-дисків, CD-R дисків) або за допомогою модему чи передавання комп'ютерною мережою".[1]

Автори науково-практичного коментаря КК 1961 року, аналізуючи статтю 198[1], яка передбачала відповідальність за розповсюдження шкідливих програмних і технічних засобів, відзначали, що подібне розповсюдження може здійснюватися шляхом: передавання програмних і технічних засобів будь-яким способом на будь-яких підставах; установки таких засобів у процесі виготовлення, ремонту, реалізації з метою подальшого використання для несанкціонованого доступу; ознайомлення інших осіб зі змістом програмних і технічних засобів, призначених для несанкціонованого доступу до інформації.[2]

Викладене дозволяє зробити висновок, що, незважаючи на розходження у визначеннях поняття розповсюдження, усі вони грунтуються, по-перше, на традиційному розумінні розповсюдження як оплатного або безоплатного передавання якогось предмета, а, по-друге, на виділенні специфічних ознак розповсюдження шкідливих програмних засобів, обумовлених особливостями предмета розповсюдження.

Саме специфіка предмета цього злочину визначає можливість його розповсюдження рядом принципово нових способів, до числа яких відносяться:

- копіювання;
- самовідтворення;
- "закладання" у програмне забезпечення;
- розповсюдження з використанням комп'ютерної мережі.

---

[1] [136] Уголовное право России. Особенная часть: Учебник /Под ред. проф. А.И. Рарога. – М.: Институт международного права и экономики им. А.С. Грибоедова, 1998. – С. 327.

[2] [92] Науково-практичний коментар Кримінального кодексу України: за станом постанов Пленуму Верховного Суду України на 1 січня 1997 р. /За ред. В.Ф. Бойка, Ю.М. Кондратьєва, С.С. Яценка. – К.: Юрінком, 1997. – С. 723 - 724.

З технічної точки зору *копіювання* являє собою "відтворення даних із збереженням вихідної інформації"[1], тобто при розповсюдженні шкідливих програм цим способом предмет розповсюдження залишається в суб'єкта злочину, а абсолютно ідентичний отримує особа, яка купує даний засіб.

Розповсюдження шкідливих програм *способом самовідтворення* означає те, що розробником передбачена можливість шкідливої програми створювати свої копії. Цей спосіб найчастіше застосовується при розповсюдженні "комп'ютерних вірусів". Комп'ютерний вірус – це параметр, який проникає в комп'ютерну програму та порушує функціювання комп'ютера, а також здатний самостійно копіювати комп'ютерні команди або заміняти програмні дані.[2] Найяскравішим прикладом комп'ютерного вірусу є так званий вірус Морріса. У листопаді 1988 року ним було уражено комп'ютерні системи Корнельського (Нью-Йорк), Стендфордського, Прінстонського (Нью-Джерсі), Гарвардського університетів, Центр Массачусетського технологічного інституту, заражено близько 1000 вузлів мережі Arpanet, серед постраждалих виявилася велика кількість урядових організацій, клінік і приватних компаній. Вірус переповнював пам'ять "зараженого" комп'ютера, чим виключав можливість роботи з інформацією, яка в ньому зберігалася. Збитки, завдані цим вірусом, оцінювалися фахівцями в 98 мільйонів доларів.[3]

Спосіб *"закладання" шкідливих програмних засобів* у програмне забезпечення полягає в тому, що особа, яка розповсюджує ці засоби, включає шкідливу програму до складу використовуваного програмного забезпечення. Один із таких способів розповсюдження шкідливих програм

---

[1] [101] Першиков В.И., Савинков В.М. Толковый словарь по информатике. – Москва: Финансы и статистика, 1991. – С. 170.

[2] [107] Положение по обеспечению безопасности компьютерных информационных систем в КНР //Борьба с преступностью за рубежом (по материалам зарубежной печати) //Ежемесячный информационный бюллетень. – М., 1996. – № 9.

[3] [64] Компьютерные террористы: новейшие технологии на службе преступного мира / Авт.-сост. Т.И. Ревяко. – Минск: Литература, 1997. – С. 327.

одержав назву "Троянський кінь". Суть його полягає в тому, що винним розповсюджується якесь корисне програмне забезпечення, наприклад, текстовий редактор, перекладач або навчальна програма, однак, крім корисних функцій, програма містить і *приховані*, призначені для порушення права власності на інформацію. Так, під час використання ігрової програми із "закладним" елементом знищуються або перекручуються всі текстові документи на жорсткому диску.

Розповсюдження шкідливих програм *способом використання комп'ютерних мереж* полягає, як правило, у розсиланні електронною поштою копій шкідливих програм. У такий спосіб розповсюджувався один із відомих вирусів останнього часу ILOVEYOU – "Я тебе кохаю". Особа одержує електронною поштою листа під назвою "Любовний лист для тебе", коли вона відкриває його, вірус сканує всі локальні й підключені мережеві диски та знищує службові файли. Після цього вірус відкриває адресну книгу в системному реєстрі та розсилає себе за всіма знайденими адресами.[1]

Слід зазначити, що можливими є комбінації названих специфічних способів розповсюдження шкідливих програмних засобів. Наприклад, розповсюдження "троянського" програмного забезпечення за допомогою електронної пошти або самовідтворення переданих електронною поштою копій шкідливих програм.

Виходячи з викладеного, можна дати таке визначення розповсюдження шкідливого програмного забезпечення: *оплатне або безоплатне передавання шкідливого програмного забезпечення, а також його копіювання, самовідтворення, "закладання" у програмне забезпечення або його розповсюдження за допомогою комп'ютерних мереж.*

Розповсюдження шкідливих технічних засобів аналогічне простому розповсюдженню матеріальних предметів. Однак і це діяння має певну

[1] [88] Милкус А. Скромный компьютерщик опаснее атомной бомбы // Комсомольская правда. – 2000. – 11 мая. – С. 3.

специфіку. Крім простого передавання таких засобів, можливе їх установлення в електронно-обчислювальні машини, системи або комп'ютерні мережі, які продаються або передаються на іншій основі, наприклад, здаються в оренду. Отже, розповсюдження шкідливих технічних засобів можна визначити таким чином: *оплатне або безоплатне передавання шкідливого технічного засобу, а також його установлення в ЕОМ, системи або комп'ютерні мережі.*

Треба зазначити ще одну особливість розповсюдження шкідливих програмних і технічних засобів. Воно може здійснюватися як за згодою особи, якій ці засоби надаються, так і без неї. У ряді випадків згода особи на одержання шкідливого програмного або технічного засобу може виключати суспільну небезпечність, а отже, караність діяння. До таких випадків слід віднести придбання шкідливих програм або технічних засобів для перевірки систем інформаційної безпеки, створення антивірусних програм, придбання даних предметів із метою проведення досліджень. Водночас кримінальна відповідальність не виключається, якщо названі засоби купуються для вчинення злочинів або правопорушень. Відсутність у особи, яка розповсюджує шкідливі програмні та технічні засоби за згодою особи, яка їх купує, відомостей про мету їх подальшого використання не виключає суспільної небезпечності, а отже – злочинності розповсюдження.

Визначаючи зміст розповсюдження шкідливих програмних або технічних засобів, необхідно торкнутися ще одного питання. Як відмічалося вище, до такого розповсюдження автори науково-практичного коментаря КК України 1961 року зараховували також ознайомлення інших осіб зі змістом цих засобів. Тобто, на їхню думку, злочинним слід визнавати розповсюдження схем технічних пристроїв, інформації про принципи їх роботи, відомостей про особливості побудови алгоритмів шкідливих програмних засобів тощо. Видається, що такі дії не відносяться до розповсюдження шкідливих програмних або технічних засобів і можуть

кваліфікуватися, за наявності відповідних суб'єктивних ознак, як пособництво у вчиненні незаконного втручання в роботу ЕОМ, систем та комп'ютерних мереж.

Слід також зазначити, що на сьогоднішній день спірним залишається питання криміналізації *створення* шкідливих програмних і технічних засобів. Наприклад, ст. 273 КК РФ, передбачає відповідальність не тільки за використання, але й за створення шкідливих програм, а в КК України відповідальність за такі діяння відсутня. Більш вдалим у цьому питанні видається українське законодавство: саме створення шкідливого програмного або технічного засобу ще не порушує суспільних інформаційних відносини і лише за наявності умислу на їх використання охоплюється приготуванням до розповсюдження даних програм. Що ж стосується використання шкідливих програм, то воно являє собою не що інше, як один із способів вчинення незаконного втручання в роботу ЕОМ, систем або комп'ютерних мереж.

Розділ 3
СУБ'ЄКТИВНІ ОЗНАКИ НЕЗАКОННОГО ВТРУЧАННЯ В РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН, СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ

3.1. Суб'єктивна сторона незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж

У статті 62 Конституції України і частині 2 статті 2 КК України закріплений принцип суб'єктивного ставлення, який обґрунтовано визнається найважливішим в оцінці законодавства демократичної та правової держави: "Особа вважається невинною у вчиненні злочину і не може бути піддана кримінальному покаранню, доки її вину не буде доведено в законному порядку і встановлено обвинувальним вироком суду".

Суворе дотримання на практиці при відправленні правосуддя цього принципу – одна з умов вирішення завдання зміцнення законності, захисту прав і свобод громадян. Тому правильно відмічено, що "психологічний аспект злочину визнається найважливішою частиною науки кримінального права та судової практики, з якою безпосередньо пов'язане вивчення причин злочинності та всіх інших питань кримінальної відповідальності й покарання".[1] Правильне встановлення суб'єктивної сторони злочину:

а) дозволяє вирішити питання про наявність або відсутність у діянні суб'єкта складу злочину;

б) виключає можливість об'єктивного ставлення[2];

в) забезпечує точну кваліфікацію злочину;

г) дає змогу відмежувати подібні за об'єктивними ознаками злочини;

---

[1] [26] Волков Б.С. Проблема воли и уголовная ответственность. – Казань: Изд-во КГУ, 1963. – С. 8.

[2] [43] Дагель П.С., Михеев Р.И. Теоретические основы установления вины: Учебное пособие. – Владивосток, 1975. – С. 12.

д) впливає на встановлення ступеня суспільної небезпечності діяння і, як наслідок, на індивідуалізацію покарання.[1]

Досліджуючи суб'єктивну сторону комп'ютерного злочину, необхідно виходити з глибоко розроблених наукою кримінального права загальних положень з цієї проблеми. Одним із таких положень є визначення суб'єктивної сторони злочину як психічного ставлення особи до вчинюваного ним суспільно небезпечного діяння та його наслідків, яке характеризується виною, мотивом, метою.[2]

Обов'язковою ознакою, яка лежить в основі принципу суб'єктивного ставлення, є вина. Саме тому можна оцінити як одне з найважливіших досягнень науки кримінального права та законотворчості передбаченість у Загальній частині КК України 2001 року норм про вину, її форми і види (Розділ V).

Стаття 23 КК визначає: "Виною є психічне ставлення особи до вчинюваної дії чи бездіяльності, передбаченої цим Кодексом, та її наслідків, виражене у формі умислу або необережності".

Об'єктивні та суб'єктивні ознаки складу злочину взаємообумовлені, нерозривно пов'язані, вони з різних боків характеризують одне й теж соціальне явище (злочин). Однак, на відміну від об'єктивних ознак складу злочину, суб'єктивна сторона відображає внутрішні процеси, що відбуваються в інтелектуальній і вольовій сферах психіки особи, яка вчиняє або готується вчинити злочин, тому з метою теоретичного аналізу складу злочину окремий розгляд ознак суб'єктивної сторони є можливим.[3]

---

[1] [138] Уголовное право. Общая часть: Учебник для вузов /Отв. ред. д-р юрид. наук, проф. И.Я. Козаченко и д-р юрид. наук, проф. З.А. Незнамова. – М.: Издательская группа ИНФРА М-НОРМА, 1997. – С. 181.

[2] [83] Курс уголовного права. Общая часть. Том 1: Учение о преступлении: Учебник для вузов /Под ред. Н.Ф. Кузнецовой, И.М. Тяжковой. – М.: Зерцало, 1999. – С. 291.

[3] [138] Уголовное право. Общая часть: Учебник для вузов /Отв. ред. д-р юрид. наук, проф. И.Я. Козаченко и д-р юрид. наук, проф. З.А. Незнамова. – М.: Издательская группа ИНФРА М-НОРМА, 1997. – С. 180.

Змістом суб'єктивної сторони є психічна діяльність особи: психічне ставлення до об'єкта, діяння та інших об'єктивних ознак скоюваного злочину. Водночас кримінально-правовий зміст поняття психічного ставлення більш вузький за загальне поняття психічної діяльності: воно містить у собі лише три ознаки – вину, мотив і мету.

Елементами вини як психічного ставлення є свідомість (інтелект) і воля, які у своїй сукупності й утворюють її зміст. Інтелектуальні ознаки відбивають пізнавальні процеси, що відбуваються у психіці особи. Вольові – характеризують свідому спрямованість діяння, прояв власної волі в досягненні певних інтересів, цілей. Різні сполучення, ступінь інтенсивності й повноти інтелектуальних і вольових ознак відбиваються законодавцем у конструюванні форм вини. У науці кримінального права досить глибоко досліджені форми вини – умисел і необережність, їх види, подібність і відмінність їх інтелектуальних і вольових ознак. Однак відсутність законодавчого визначення видів умислу та необережності призводило раніше до серйозних недоліків у практиці оцінки суб'єктивної сторони конкретних злочинів: суди в більшості випадків обмежувалися вказівкою на форму вини без позначення її виду. Водночас уже достатньо доведено й обґрунтовано, що врахування видів умислу та необережності є важливою умовою вирішення питання про злочинність діяння, наявність складу злочину, його кваліфікацію, застосування різних інститутів кримінального права (наприклад, замаху, співучасті), призначення покарання. Тому безсумнівною позитивною якістю КК України 2001 року є передбаченість у ньому не тільки форм, але й видів вини, їх змісту, що є важливою ґарантією правильної кваліфікації скоєного злочину, а отже, правильного визначення його кримінально-правових наслідків.

Викладене є вагомим арґументом для висновку про те, що, досліджуючи будь-який склад злочину, недостатньо визначати його об'єкт та об'єктивну сторону. Без з'ясування суб'єктивної сторони і, насамперед,

форми й виду вини, не можна зробити однозначний висновок про наявність цього складу.

Складність встановлення суб'єктивної сторони зумовлена тим, що, на відміну від об'єктивної сторони, вона є внутрішньою стороною злочину, яка не лежить на поверхні вчиненого. Крім того, законодавець рідко в диспозиції вказує на форму та вид вини.

Ураховуючи, що суб'єктивна сторона є відображенням у психіці особи об'єкта й об'єктивної сторони конкретного злочину, в аналізі суб'єктивної сторони незаконного втручання необхідно виходити з викладеної характеристики змісту його об'єкта та об'єктивної сторони. Як уже зазначалося, втручання – це свідома зміна режиму роботи електронно-обчислювальних машин, систем та комп'ютерних мереж шляхом використання закономірностей їх функціонування. Виходячи з етимології терміна "втручання", вина в цьому складі може бути виражена тільки в умислі. Але цього недостатньо: відповідно до закону необхідним є встановлення й обгрунтування його виду.

Специфіка об'єктивної сторони двох форм незаконного втручання, перша з яких є злочином з матеріальним, а друга – з формальним складом, дозволяє зробити висновок про те, що зміст умислу в них може бути різним.

1. При скоєнні досліджуваного злочину у *формі незаконного втручання* в роботу електронно-обчислювальних машин, систем або комп'ютерних мереж, яке спричинило знищення або перекручення інформації (матеріальний склад), суб'єктивна сторона виражається в тому, що особа: а) усвідомлювала суспільну небезпечність незаконного втручання, тобто фактичні та соціальні ознаки діяння, його протиправність; б) передбачала наслідки у вигляді знищення або перекручення комп'ютерної інформації; в) бажала або свідомо припускала настання цих наслідків. Тобто суб'єктивна сторона аналізованого складу в цій формі може виражатися у

вигляді як прямого, так і непрямого умислу. Це підтверджується такими положеннями.

Загальною ознакою інтелектуального моменту прямого та непрямого умислу є усвідомлення суспільної небезпечності діяння, під яким у науці кримінального права обґрунтовано розуміється: усвідомлення фактичних об'єктивних ознак вчиненого діяння та усвідомлення його соціального значення – суспільної небезпечності.[1] Усвідомлення фактичних ознак незаконного втручання полягає в тому, що особа усвідомлює закономірності функціонування ЕОМ, системи або комп'ютерної мережі, використання яких дозволяє здійснювати втручання в їх роботу. Дослідження цієї ознаки суб'єктивної сторони робить необхідним встановлення меж усвідомлення особою використовуваних закономірностей. Зрозуміло, що вимога усвідомлення об'єктивних ознак незаконного втручання як точного, всебічного знання про всі процеси, що відбуваються в ЕОМ під час незаконного втручання, буде неправильною. Це пов'язано з тим, що функціонування ЕОМ – це надзвичайно складний і багатоплановий процес. Тому особа, яка здійснює незаконне втручання, не обов'язково повинна усвідомлювати всі деталі цього процесу. Наприклад, те, що в результаті натиснення нею кнопки сигнал із клавіатури комп'ютера буде опрацьовано контролером введення-виведення та направлено у центральний процесор, який цього часу виконуватиме завдання, котрі знаходяться в оперативному пристрої комп'ютера, і що процесор, опрацювавши цей сигнал відповідно до виконуваної програми, знову через контролер введення-виведення спрямує команду накопичувачу інформації (наприклад, дисководу для гнучких або жорстких магнітних дисків.), де у свою чергу голівка читання-запису займе положення, відповідне до фізичного розташування на носії інформації, що знищується або перекручується, і шляхом моделювання напруженості

[1] [42] Дагель П.С., Котов Д.П. Субъективная сторона преступления и ее установление. – Воронеж, 1974. – С. 85.

електромагнітного поля комп'ютерна інформація буде знищена або перекручена. На сьогодні досягнення у сфері виробництва апаратних засобів і програмного забезпечення призвели до ситуації, коли детальне знання про процеси, що відбуваються під час роботи ЕОМ, не є обов'язковим для виконання завдань опрацювання інформації з застосуванням комп'ютерної техніки. Видається, що для підтвердження цього висновку цілком прийнятна позиція А.Н. Трайніна, який писав, що для наявності умислу цілком достатньо, щоб особа в *основних рисах* усвідомлювала перебіг і зв'язок подій, які призводять до злочинного результату.[1] Таким чином, усвідомлення фактичних об'єктивних ознак незаконного втручання полягає в розумінні в основних рисах загальних закономірностей функціонування ЕОМ, тобто достатньо наявності в особи знань про те, що певні дії порушать правильну роботу ЕОМ, системи або комп'ютерної мережі, і можуть призвести до перекручення чи знищення інформації.

Важливою складовою інтелектуального моменту незаконного втручання є усвідомлення особою протиправності своїх дій. Хоча усвідомлення протиправності у визначенні видів умислу законодавцем не вказується як обов'язкова ознака, що значною мірою зумовлено конституційним принципом – незнання закону не виключає кримінальної відповідальності, але в деяких складах злочину таке усвідомлення є обов'язковим. Саме таким складом є незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж: указуючи на незаконність як обов'язкову ознаку об'єктивної сторони, законодавець вимагає усвідомлення винним незаконності (протиправності) втручання. Усвідомлення протиправності в цьому складі злочину зумовлене насамперед розумінням об'єкта незаконного втручання, яким, як зазначалося вище, виступає право власності на чужу комп'ютерну

інформацію. Отже, суб'єкт злочину знає про відсутність у нього такого права, розуміє, що він порушує встановлений власником інформації порядок використання електронно-обчислювальних машин, систем та комп'ютерних мереж, і що це закономірно спричиняє перекручення або знищення чужої інформації. Наявність у особи права на інформацію або наявність у нього помилкового уявлення про те, що таке право йому належить, виключає відповідальність за порушення права власності на комп'ютерну інформацію. У деяких випадках, за наявності необхідних ознак, такі дії можуть містити склади інших злочинів (наприклад, самоправства – ст. 356 КК).

Усвідомлення протиправності нерозривно пов'язане з усвідомленням суспільної небезпечності: розуміючи, що порушує нормативні приписи, суб'єкт неминуче усвідомлює суспільну небезпечність свого діяння. З іншого боку, не усвідомлюючи суспільної небезпечності, суб'єкт не усвідомлює і протиправності діяння. На підтвердження цього можна навести такий приклад. М., співробітник підприємства "М-софт", яке займається виробництвом програмного забезпечення, звернувся до Н. по допомогу в розробленні нового додатка. Н., бажаючи заподіяти шкоду підприємству "М-софт", розробляє необхідний М. додаток і встановлює в ньому приховану функцію. Ця функція полягає в тому, що коли розроблений Н. додаток починає виконуватися на електронно-обчислювальній машині підприємства "М-софт", уся інформація, яка зберігається в ній, знищується. Не знаючи цього, М. встановив розроблений Н. додаток на одному з комп'ютерів фірми "М-софт" і, запустивши його, знищив комп'ютерну інформацію, яка зберігалася в машині. Зрозуміло, що ці дії М. не були усвідомленими в кримінально-правовому розумінні: М. не усвідомлював, що своїми діями він здійснює незаконне втручання в роботу електронно-

[1] [134] Трайнин А.Н. Состав преступления по советскому уголовному праву. – М.: Государственное издательство юридической литературы, 1951. – С. 218.

обчислювальних машин, а, отже, не усвідомлював і суспільної небезпечності вчинюваних ним дій.

Обов'язковою інтелектуальною ознакою прямого умислу є передбачення особою суспільно-небезпечних наслідків своїх дій. Як справедливо відмічає Н.Ф. Кузнєцова, передбачення наслідків при вчиненні злочину з прямим умислом може бути двояким: "…винний передбачає можливість або неминучість настання суспільно небезпечних наслідків".[1] Зазначені варіанти передбачення при прямому умислі можливі й у складі незаконного втручання в роботу ЕОМ.

Передбачення *неминучості* знищення або перекручення комп'ютерної інформації виявляється в розумінні винним закономірностей зв'язку між його незаконним втручанням і знищенням або перекрученням комп'ютерної інформації. Особа, яка здійснює незаконне втручання, передбачає, що в результаті вчинюваних нею дій інформація обов'язково буде знищена або перекручена і можливість власника здійснювати свої правомочності буде виключена або значно обмежена. Передбачення неминучості настання суспільно-небезпечних наслідків незаконного втручання в роботу електронно-обчислювальних машин, систем або комп'ютерних мереж буде мати місце, наприклад, у випадку втручання, здійснюваного шляхом використання стандартного інтерфейсу користувача. У цьому випадку для знищення інформації може використовуватися стандартний додаток операційної системи Windows – "Провідник". Особа за допомогою цієї програми знищує файли, що містять комп'ютерну інформацію, і після цієї операції очищує список нещодавно видалених файлів ("кошик"). Ці нескладні операції з необхідністю спричиняють знищення комп'ютерної інформації та виключають можливість відновлення знищених файлів.

---

[1] [83] Курс уголовного права. Общая часть. Том 1: Учение о преступлении: Учебник для вузов /Под ред. Н.Ф. Кузнецовой, И.М. Тяжковой. – М.: Зерцало, 1999. – С.309.

Передбачення *реальної можливості* настання суспільно небезпечних наслідків незаконного втручання наявне у випадку, якщо воно здійснюється з використанням засобів спеціального технічного впливу (цей спосіб вчинення незаконного втручання був описаний при дослідженні об'єктивної сторони). Застосування для знищення або перекручення інформації електромагнітного випромінювання не забезпечує неминучого настання суспільно небезпечних наслідків, однак створює їх реальну можливість.

Вольовий момент прямого умислу при вчиненні незаконного втручання полягає в бажанні знищити або перекрутити комп'ютерну інформацію. Про його наявність можуть свідчити характер дій, спосіб вчинення незаконного втручання та мета, якою керується особа.

Обґрунтованою в науці кримінального права є позиція про те, що усвідомлення суспільної небезпечності діяння є загальною ознакою прямого та непрямого умислу. Відмінності ж полягають у *характері* передбачення суспільно небезпечних наслідків та змісті вольового моменту. При вчиненні незаконного втручання з непрямим умислом особа передбачає лише можливість, імовірність настання наслідків у вигляді знищення або перекручення комп'ютерної інформації. Передбачення неминучості настання цих наслідків завжди буде свідченням того, що особа бажає настання наслідків, тобто діє з прямим умислом.

Відмінність непрямого та прямого умислу в характеристиці їх вольового моменту полягає в тому, що при скоєнні злочину з непрямим умислом особа, хоча й не бажала, але свідомо припускала настання суспільно небезпечних наслідків, що може виражатися в байдужому до них ставленні або в розрахунку на обставини, які об'єктивно не можуть запобігти таким наслідкам. Як правило, це відбувається в результаті того, що особа керується метою, яка лежить *за межами* цього складу. Прикладом вчинення незаконного втручання з непрямим умислом може бути такий випадок. Особа, маючи за мету одержати для подальшого використання

відомості, що становлять комерційну таємницю, здійснює незаконне втручання в роботу електронно-обчислювальної машини, свідомо припускаючи можливість знищення або перекручення комп'ютерної інформації. У результаті такого втручання особа одержала інформацію, яка її цікавить, а певна комп'ютерна інформація була знищена. У цьому випадку в діях особи має місце сукупність злочинів: незаконне втручання з непрямим умислом і незаконне збирання з метою використання відомостей, що становлять комерційну таємницю, яке вчинюється з прямим умислом (ст. 231 КК України).

2. *Розповсюдження шкідливих програмних або технічних засобів* – друга форма незаконного втручання, як вже було відзначено, відноситься до злочинів із формальним складом. Виходячи з цього, зміст її суб'єктивної сторони визначається лише психічним ставленням до діяння і полягає в усвідомленні суспільної небезпечності та протиправності розповсюдження шкідливих програмних і технічних засобів та бажанні вчинення таких дій. Отже, у цій формі умисел може бути тільки прямим, а його специфіка виражається в тому, що свідомістю особи обов'язково охоплюється розуміння того, що розповсюджувані засоби *спеціально призначені для незаконного втручання в роботу електронно-обчислювальних машин, систем або комп'ютерних мереж.*

Обов'язковою ознакою суб'єктивної сторони цього комп'ютерного злочину є усвідомлення особою специфічних властивостей та призначення технічних і програмних засобів, які вона розповсюджує. У випадку, якщо особа не усвідомлює властивостей програмних або технічних засобів, розповсюджуваних нею, виключається кримінальна відповідальність за їх розповсюдження. У цьому розумінні показовим є приклад розповсюдження шкідливих програм під виглядом нового програмного забезпечення. Особа розробляє програму з прихованою шкідливою функцією та подає її для загального користування в комп'ютерну мережу. Крім того, вона готує

повідомлення, у якому пропонує, наприклад, за винагороду, розповсюджувати цю програму всім, хто її скопіював. У такому випадку кримінальна відповідальність осіб, які скопіювали цю програму й розповсюджують її, виключається через відсутність усвідомлення ними шкідливих властивостей предмета злочину. Якщо ж особа помилялася стосовно властивостей розповсюджуваних програмних або технічних засобів, тобто вважала їх шкідливими, але вони такими не були, відповідальність повинна наставати за замах на розповсюдження шкідливих програмних і технічних засобів.

Усвідомлення діяння як складовий елемент суб'єктивної сторони розповсюдження шкідливих програмних або технічних засобів полягає в розумінні особою того, що в результаті її дій використання шкідливих засобів стає можливим для іншої особи або певної кількості осіб.

Значний інтерес в аналізі суб'єктивної сторони незаконного втручання становить дослідження її факультативних ознак – мотиву та мети злочину. Загальновизнано, що мотив злочину – це "внутрішнє спонукання, рушійна сила вчинку людини"[1], якою керувалась особа, вчиняючи злочин; мета злочину – це уявлення про той результат, якого прагне досягти особа, вчиняючи суспільно небезпечне діяння.[2] Мотив і мета, не будучи обов'язковими ознаками суб'єктивної сторони незаконного втручання, впливають на ступінь суспільної небезпечності злочину та особи, яка його вчинила, а тому вимагають обов'язкового встановлення.

Як свідчить досвід боротьби з комп'ютерними злочинами в Україні та за рубежем, найпоширенішим мотивом вчинення незаконного втручання є користь, тобто бажання незаконного збагачення. Існує думка, що близько

---

[1] [71] Кримінальне право України: Загальна частина: Підручник для студентів юрид. спец. вищ. закладів освіти /М.І. Бажанов, Ю.В. Баулін, В.І. Борисов та ін.; За ред. професорів М.І. Бажанова, В.В. Сташиса, В.Я. Тація. – Київ-Харків: Юрінком Інтер-Право, 2001. – С. 162.

[2] [25] Волков Б.С. Мотивы преступлений (Уголовно-правовое и социально-психологическое исследование). – М.: Издательство Казанского университета, 1982. – С. 6-7.

80% комп’ютерних злочинів вчиняються саме з корисливих мотивів. Наступним за поширеністю мотивом вчинення незаконного втручання, на думку автора, є самоствердження. Іноді ті, хто вивчає програмування, доходять висновку, що кращим засобом перевірки їх знань є "злом" будь-якої захищеної системи або розроблення та випуск шкідливої програми. Як приклад такої мотивації видається можливим навести один із перших у світовій практиці випадків розповсюдження шкідливих програм. У 1988 році в США тисяча комп’ютерів припинили роботу, зупинилася робота багатьох підприємств, установ та організацій, завдані збитки оцінювалися кількома мільйонами доларів. Причиною цих подій стала шкідлива комп’ютерна програма "черв'як", розроблена студентом Корнельского університету Робертом Моррісом. На попередньому розслідуванні було встановлено, що своїми діями Морріс бажав показати виявлену ним недосконаліть діючих на той час систем інформаційної безпеки. Крім самоствердження деякі автори виокремлюють також такі мотиви вчинення комп’ютерних злочинів як помста за образу, бажання “пожартувати” та ігнорування етики.[1]

Певну специфіку має характеристика мети як однієї з ознак суб’єктивної сторони незаконного втручання. Цілі можуть бути різними. Водночас, якщо незаконне втручання здійснюється, наприклад, з метою заподіяння шкоди інформаційній безпеці України, то дії особи слід кваліфікувати не за ст. 361 КК України, а як державну зраду (ст. 111 КК) або шпигунство (ст. 114).

3.2. Суб’єкт незаконного втручання в роботу електронно-обчислювальних машин, систем та комп’ютерних мереж

[1] [76] Крылов В.В. Информационные компьютерные преступления. – М.: Издательская группа Инфра М-Норма, 1997. – С. 65; [9] Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юридическая литература, 1991. – С 43.

Серед проблем кримінальної відповідальності за комп'ютерні злочини питання, які стосуються суб'єкта цих злочинів, найчастіше висвітлювалися в літературі тільки з точки зору їх кримінологічної характеристики. Поширеною є думка про те, що часто комп'ютерні злочини скоюються неповнолітніми – школярами, які успішно вивчають інформатику, і що комп'ютерний злочинець – хакер – це людина, яка володіє серйозними знаннями у сфері комп'ютерних технологій тощо. Пропонуються різні класифікації цих суб'єктів. Наприклад: пірати порушують головним чином авторське право, створюючи незаконні версії програм і даних; хакери одержують неправомірний доступ до комп'ютерів інших користувачів і файлів у них; кракери – це найбільш серйозні порушники.[1] Висловлювалася думка, що хакерів слід класифікувати так: "крекери – фахівці з обходу механізмів безпеки; кранчери – фахівці зі зняття з програмного забезпечення захисту від копіювання; крешери – аматори активно поекспериментувати з комп'ютерною системою з метою з'ясування можливостей керування нею".[2] Називаються також такі групи суб'єктів комп'ютерних злочинів, як софтверні хакери – займаються "зломом" програмного забезпечення, мережні хакери – основний рід діяльності полягає в неправомірному одержанні платних послуг провайдерів, одержанні неправомірного доступу до комп'ютерних систем без відповідних повноважень.[3] Деякі автори виокремлюють наступні типи "комп'ютерних" злочинців:

1. Порушники правил користування ЕОМ. Вони вчиняють злочини внаслідок недостатнього знання техніки, бажання ознайомитися з

[1] [78] Кузнецов А. Пираты в Интернете //Милиция. – 2000. – № 2. – С. 27
[2] [64] Компьютерные террористы: новейшие технологии на службе преступного мира /Авт.-сост. Т.И. Ревяко. – Минск: Литература, 1997. – С. 115.
[3] [64] Там само. – С. 125-131.

інформацією, яка їх цікавить, викрасти яку-небудь програму чи безкоштовно користуватися послугами електронно-обчислювальних машин.

2. "Білі комірці" – так звані респектабельні злочинці: бухгалтери, управляючі фінансами різноманітних фірм, адвокати, віце-президенти компаній і т.п. Для них характерні такі дії, як використання комп'ютера з метою моделювання злочинів, що плануються, комп'ютерний шантаж конкурентів, фальсифікація інформації і т.д. Метою таких дій є отримання матеріальної вигоди або приховування інших злочинів.

3. "Комп'ютерні шпигуни". Вони представляють собою добре підготовлених у технічному та організаційному відношенні фахівців. Їх метою є отримання стратегічно важливих даних про супротивника в економічній, технічній та інших галузях.

4. "Хакери". Ця категорія осіб є найбільш технічно та професійно підготовленою, вони відмінно розбираються в обчислювальній техніці та програмуванні. Їх діяльність направлена на несанкціоноване проникнення в комп'ютерні мережі, крадіжку, модифікацію або знищення інформації що в них знаходиться. Дуже часто вони скоюють злочини, не переслідуючи при цьому прямих матеріальних вигод.[1]

Усі ці характеристики, безумовно, мають значення для конкретизації ролі даних суб'єктів, характеру їх діянь, суспільної небезпечності, однак вони не вирішують питання про ознаки суб'єкта злочину як елемента складу незаконного втручання, не розкривають його юридичних ознак, кримінально-правової характеристики.

Між тим кваліфікація цих злочинів, у тому числі і незаконного втручання, передбачає вирішення питання саме про юридичні ознаки. Стаття 18 КК України 2001 року в ч. 1 вперше на законодавчому рівні дає визначення загального суб'єкта злочину: "Суб'єктом злочину є фізична

[1] [65]Компьютерные технологии в юридической деятельности. Учебное и практическое пособие / Под ред. Н.Полевого, В. Крылова. - М., 1994. - С 64.

осудна особа, яка вчинила злочин у віці, з якого відповідно до цього Кодексу може наставати кримінальна відповідальність.” Таким чином, суб'єктом будь-якого злочину (якщо інше не передбачено законом) може бути людина, яка досягла певного віку і яка на час вчинення злочину могла усвідомлювати свої дії (бездіяльність) і керувати ними. Ця характеристика суб'єкта повністю поширюється на суб'єкта незаконного втручання, оскільки ст. 361 не містить ніяких особливих його ознак. Однак деякі питання щодо ознак суб'єкта незаконного втручання потребують дослідження, а саме: вік суб'єкта та проблема спеціального суб'єкту.

Що стосується віку суб'єкта незаконного втручання, то згідно зі ст. 22 КК, ним є загальний вік – шістнадцять років. Законодавець, виходячи зі складності об’єктивної сторони, характеру й ступеня небезпечності злочину, не визнав за можливе знизити вік суб’єкта комп’ютерного злочину. Однак таке рішення не завжди оцінюється однозначно. Досить поширеною є думка про те, що часто комп’ютерні злочини вчинюються особами, які не досягли шістнадцяти років, тому встановлення загального віку кримінальної відповідальності за ці злочини може призвести до неефективності механізму кримінально-правового захисту інформаційних відносин.

Достатньо обгрунтовано, що підставою для зниження законодавцем віку кримінальної відповідальності за певні злочини є сукупність таких критерієв:

1) певний рівень розумового розвитку, свідомості особи, який свідчить про можливість уже в чотирнадцять років усвідомлювати суспільну небезпечність і протиправність злочинів;

2) значна поширеність серед підлітків;

3) значна суспільна небезпечність (тяжкість) злочинів.[1]

[1] [71] Кримінальне право України: Загальна частина: Підручник для студентів юрид. спец. вищ. закладів освіти /М.І. Бажанов, Ю.В. Баулін, В.І. Борисов та ін.; За ред. професорів М.І. Бажанова, В.В. Сташиса, В.Я. Тація. – Київ-Харків: Юрінком Інтер-Право, 2001. – С. 132.

Саме з цих критерієв слід виходити, вирішуючи питання про доцільність або недоцільність зниження віку суб'єкта незаконного втручання.

По-перше, слід зазначити, що хоча комп'ютерні злочини, вчинені особами, які не досягли шістнадцяти років, дійсно можуть заподіяти тяжкі наслідки, особа неповнолітнього характеризується певною специфікою: насамперед їй притаманна зацікавленість самим процесом роботи з комп'ютерною технікою, бажання виявити свої здібності в керуванні складною технікою. Усвідомлення можливості заподіяння шкоди власнику інформації, а отже усвідомлення суспільної небезпечності, протиправності втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж не сприймається в більшості випадків як реально можливий і бажаний результат. Так, 15-річний громадянин Хорватії Віце Мешкович, бажаючи показати своє вміння, здійснював неодноразовий несанкціонований доступ до комп'ютерної інформації, що належала ВВС США.[1] В одному з офіційних повідомлень Міністерства юстиції США йшлося про затримання неповнолітнього, який з тією ж метою використовував комп'ютер для виведення з ладу контрольної вежі аеропорту в Бостоні.[2]

По-друге, що стосується такого критерію, як поширеність комп'ютерних злочинів серед неповнолітніх, котрі не досягли шістнадцятирічного віку, то статистичні дані не підтверджують цей висновок. На жаль, в Україні не має такої статистики, однак дослідження зарубіжних кримінологів показали, що вік 33% осіб на момент скоєння комп'ютерного злочину не перевищував 20 років, 54% мали вік від 20 до 40

[1] [64] Компьютерные террористы: новейшие технологии на службе преступного мира /Авт.-сост. Т.И. Ревяко. – Минск: Литература, 1997. – С. 257 – 258.

[2] [164] Juvenile Computer Hacker Cuts off FAA Tower at Regional Airport – First Federal Charges Brought Against a Juvenile for Computer Crime (March 18, 1998), http://www.usdoj.gov/crimrnal/cybercrime/juvenilepld.html

років, а 13 % - більше 40 років.[1] А. Кузнєцов наводить дані про те, що половина хакерів, заарештованих у США, мають вік від 25 до 30 років і лише сьома частина – до 21 року.[2] На думку російських дослідників, більшість хакерів – особи віком від 16-17 до 20-25 років. В цьому віці здатність до сприймання інформації найбільш висока, що особливо важливо для комп'ютерних злочинів.[3] Отже, обґрунтованим буде висновок про те, що вчинення незаконного втручання особами, які не досягли шістнадцяти років, не є значно поширеним.

Усе це свідчить про відсутність тих критеріїв, що могли б зумовити підвищений ступінь суспільної небезпечності незаконного втручання, вчиненого особою, яка не досягла шістнадцяти років, і про можливість її виправлення іншими, не кримінально-правовими, заходами, а, отже, дозволяє зробити висновок про недоцільність зниження вікової межі суб'єкта комп'ютерних злочинів до чотирнадцяти років.

Таким чином, встановлення в ст. 22 КК України загального віку кримінальної відповідальності за комп'ютерні злочини видається соціально обґрунтованим.

Друга проблема суб'єкта незаконного втручання, яка становить значний інтерес і потребує вирішення, пов'язана з питанням спеціального суб'єкта. В літературі досить поширеною є така класифікація суб'єктів незаконного втручання: а) особи, які знаходяться в трудових відносинах з підприємством, організацією, установою, фірмою чи компанією, в якій вчинено злочин (особи, які безпосередньо займаються обслуговуванням електронно-обчислювальних машин: оператори, програмісти, інженери, персонал, який займається технічним обслуговуванням та ремонтом

---

[1] [16] Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп'ютерна злочинність: Навчальний посібник. – К.: Атіка, 2002. – С. 123.
[2] [78] Кузнецов А. Пираты в Интернете //Милиция. – 2000. – № 2. – С.27
[3] [114]Расследование неправомерного доступа к компьютерной информации / Под. ред. Н.Г. Шуруханова. – М.: Щит – М, 1999. – С. 123.

комп’ютерної техніки); користувачі електронно-обчислювальних машин, які мають певну підготовку та вільний доступ до комп’ютерної системи; адміністративно-керівничий персонал (керівники, бухгалтери, економісти)); б) особи, які не знаходяться в трудових відносинах з підприємством, організацією, установою, фірмою чи компанією, в якій вчинено злочин.[1] Як свідчить практика зарубіжних правоохоронних органів, досить часто комп'ютерні злочини, у тому числі незаконне втручання, вчиняються суб’єктами, які відносяться саме до першої групи, тобто за посадами або за характером обов'язків безпосередньо пов'язані з доступом до роботи з електронно-обчислювальними машинами, системами та комп'ютерними мережами.

Так, Роберт Кортні, консультант із питань безпеки в корпорації Ай-Бі-Ем, відзначає, що лише 3 % порушень інформаційної безпеки пов’язані з діяльністю осіб, які не мають певного відношення до діяльності конкретних підприємств, компаній; інші 97% порушень вчиняються їх службовцями.[2] Спеціальні дослідження американських правоохоронних органів щодо порушень інформаційної безпеки в Національному центрі кримінальної інформації (National Crime Information Center) показали, що більшість таких порушень вчинено службовцями цієї організації.[3] Одне з перших незаконних втручань у роботу електронно-обчислювальних машин, що мало місце в Україні, було також вчинено працівником потерпілої організації. З вересня по грудень 1999 року в Донецьку (досудове слідство провадилося

---

[1] Див.: [86]Лысов Н.Н. Содержание и значение криминалистической характеристики компьютерных преступлений // Проблемы криминалистики и методики ее преподавания (тезисы выступлений участников семинара-совещания преподавателей криминалистики). – М., 1994. – С. 54.; [159] Шилан Н.Н., Кривонос Ю.М., Бирюков Г.М. Компьютерные преступления и проблемы защиты информации: Монография – Луганск: РИО ЛИВД, 1999. – С. 38.

[2] [64] Компьютерные террористы: новейшие технологии на службе преступного мира /Авт.-сост. Т.И. Ревяко. – Минск: Литература, 1997. – С. 219.

[3] [166] The National Information Infrastructure Protection Act of 1996 Legislative Analysis By The Computer Crime and Intellectual Property Section United States Department of Justice, http://www.usdoj.gov/criminal/cybercrime /1030_anal.html.

прокуратурою Донецької області) головний інженер-електронник Центру інформаційних технологій і технічного забезпечення Донецької дирекції Українського Державного підприємства електрозв'язку "Укртелеком" розробив комп'ютерну програму, яка дозволяє відшукувати в масиві фіксованої структури телефонні розмови, проведені з заданих номерів телефонів, відбирати їх та стирати інформацію про них у даному масиві. Винний увійшов у змову з громадянином Пакистану, який навчався в Донецьку та залучав клієнтів. Спільно вони надавали їм за заниженими тарифами послуги міжнародного та міжміського телефонного зв'язку, а інформацію про переговори, що здійснювалися клієнтами, знищували за допомогою програми, розробленої інженером-програмістом. Внаслідок таких дій підприємству електрозв'язку був заподіяно збитки у розмірі близько 150 тисяч гривень.

Про те, що більшість злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж вчиняються працівниками підприємств, установ чи організацій, які постраждали, свідчать і результати експертних опитувань працівників служб безпеки. На їхню думку, найбільша небезпека в плані вчинення комп'ютерних злочинів "виходить саме від безпосередніх користувачів, і ними вчиняється 94% злочинів, тимчасом як опосередкованими користувачами – тільки 6%".[1] *Таким чином, практика боротьби з комп'ютерними злочинами свідчить про підвищену небезпечність цих злочинів у випадку їх вчинення особою, яка має доступ до ЕОМ, системи або комп'ютерної мережі у зв'язку з займаною посадою або спеціальними повноваженнями.*

Здебільшого в ролі спеціального суб'єкта комп'ютерного злочину виступає особа, яка має правомірний доступ до комп'ютерної інформації, що є предметом незаконного втручання, але більшість цих осіб не

[1] [16] Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп'ютерна злочинність: Навчальний посібник. – К.: Атіка, 2002. – С. 131.

здійснюють функцію представника влади, не займають посади, пов’язані з виконанням організаційно-розпорядчих чи адміністративно-господарських обов'язків, тобто не є службовими особами. Отже, і вчинені ними дії додатковій кваліфікації за статтями КК, що передбачають відповідальність за злочини в сфері службової діяльності, не підлягають.

Таким чином, у більшості випадків, коли незаконне втручання вчиняється особою, яка має правомірний доступ до комп’ютерної інформації, що є предметом злочину, і це значно підвищує ступінь суспільної небезпечності даного злочину, її дії кваліфікуватимуться як простий склад незаконного втручання. Таке положення, коли кваліфікація злочину не відповідає ступеню його суспільної небезпечності, свідчить про певну недосконаліть діючого механізму кримінально-правової охорони суспільних відносин власності на комп’ютерну інформацію від незаконного втручання в роботу електронно-обчислювальних машин.

Виходячи з цього, видається доцільним доповнити ч. 2 ст. 361 КК України додатковою кваліфікуючою ознакою*: вчинення незаконного втручання особою, яка має правомірний доступ до ЕОМ, систем або комп’ютерних мереж у зв’язку з займаною посадою або спеціальними повноваженнями.*

До таких осіб слід зараховувати робітників підприємств, установ або організацій, функціональні обов’язки яких передбачають використання комп’ютерної інформації, що належить роботодавцю, для виконання завдань, які стоять перед ними (інженери-програмісти, оператори ЕОМ, адміністратори комп’ютерних мереж тощо). Важливо відмітити, що ознаки спеціального суб’єкта незаконного втручання мають тільки безпосередні користувачі ЕОМ, систем або комп’ютерних мереж. Допоміжний персонал (водії, охоронці, слюсарі тощо) хоча і може мати певний доступ до ЕОМ, системи або комп’ютерної мережі, до спеціальних суб’єктів незаконного втручання не належить через те, не має санкціонованого доступу.

Розділ 4
КВАЛІФІКУЮЧІ ОЗНАКИ НЕЗАКОННОГО ВТРУЧАННЯ В РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН, СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ

4.1. Незаконне втручання, що заподіяло істотну шкоду

Необхідно відмітити, що незаконне втручання в роботу електронно-обчислювальних машин, яке заподіяло істотну шкоду, відноситься до так званих злочинів, що кваліфікуються за наслідками. Аналізуючи такі злочини, М.І. Бажанов відзначав: "… у всіх злочинах, що кваліфікуються за наслідками, є два наслідки – основний (проміжний) і додатковий (похідний). Ці наслідки настають хронологічно (послідовно) один за одним, у результаті вчинення особою діяння … Причому основний (проміжний) наслідок тягне за собою додатковий (похідний), оскільки приховує в собі реальну можливість настання цього похідного наслідку. Діяння безпосередньої "участі" у настанні додаткового наслідку не бере. Воно породжує проміжний наслідок, який, у свою чергу, викликає наслідок похідний".[1]

В аналізованому злочині основний наслідок полягає у знищенні або перекрученні комп'ютерної інформації, а додатковий – у заподіянні істотної шкоди. Виходячи з того, що законодавець не розкриває змісту цієї кваліфікуючої ознаки, можна зробити висновок: поняття істотної шкоди в цьому складі є оціночним. На відміну від понять точного значення, такі

[1] [4] Бажанов М.И. Множественность преступлений по уголовному праву Украины. – Х.: Право, 2000. – С. 23.

поняття характеризуються невизначеністю, відсутністю однозначних, чітких, суворо фіксованих ознак.[1]

Виступаючи однією з проблем загальної теорії права, оціночні поняття привернули серйозну увагу і в науці кримінального права. Видається правильним визначення оціночних понять, запропоноване А.В. Наумовим: "Оціночні поняття в кримінально-правових нормах – це ті ознаки складу злочину, що визначаються не законом або іншим нормативним актом, а правосвідомістю особи, яка застосовує відповідну правову норму, виходячи з конкретних обставин справи".[2]

Специфіка оціночних понять у тому, що, "формулюючи таке поняття в законі, законодавець не розкриває повністю його змісту, він називає лише одну або декілька найбільш загальних властивостей, які виражають основний зміст класу явищ, надаючи правозастосовчим органам право, по-перше, визначати обсяг цього класу, по-друге, розкривати зміст самого даного в законі поняття відбиттям інших істотних ознак".[3]

Необхідність застосування законодавцем оціночних понять обумовлена, насамперед, різноманітністю явищ, що потребують кримінально-правової охорони, і стрімкою зміною життєвих умов. Водночас "ці поняття, будучи високоабстрактними, дають можливість законодавцю включати до сфери правового реґулювання більшу кількість явищ, предметів, станів, які відрізняються різними емпіричними властивостями".[4] "У використанні таких понять відбито прагнення законодавця дати суб’єкту застосування кримінально-правової норми

---

[1] [99] Панов Н.И. Оценочные понятия и их применение в уголовном праве //Проблемы социалистической законности: Республ. межвед. научн. сб. – Вып. 7. – Х.: Вища школа, 1981. – С. 99.

[2] [93] Наумов А.В. Применение уголовно-правовых норм. – Волгоград: 1973. – С.97.

[3] [68] Кривоченко Л.Н. Классификация преступлений. – Х.: Издательство при Харьковском государственном университете издательского объединения "Вища школа", 1983. – С. 35-36.

[4] [104] Питецкий В. Конкретизация оценочных признаков уголовного законодательства //Советская юстиция. – 1991. – № 2. – С. 12-13.

можливість максимально врахувати фактичні обставини конкретної справи, а також вимоги мінливих умов життя суспільства".[1]

При цьому характерною особливістю оціночних понять є те, що термінологічний їх збіг у різних складах злочинів не означає тотожності їх за змістом. Ще в 1988 році В. Питецький правильно підкреслював, що "те саме оціночне поняття, будучи використаним у різних статтях кримінального кодексу, як правило, має різний зміст, охоплює різний обсяг явищ. Тобто термінологічний збіг оціночних ознак не є їх збігом за змістом та обсягом … Тому при встановленні змісту оціночних понять велике значення має врахування місця знаходження останніх у системі норм КК, конкретних обставин справ, особливостей об'єкта посягання та інших чинників".[2]

Викладені характеристики оціночних понять і покладені в основу аналізу істотної шкоди як кваліфікуючої ознаки незаконного втручання, з урахуванням його місця в системі КК, специфіки його об'єкта, предмета, об'єктивної та суб'єктивної сторін.

Особливе значення для цього аналізу має додатковий об'єкт. Відомо, що у злочинах, які кваліфікуються за наслідками, додатковим об'єктом, як правило, є більш важливі суспільні відносини, цінності, блага, ніж ті, які утворюють основний об'єкт.[3] Саме зміст додаткового об'єкта, його цінність у системі суспільних відносин значною мірою впливають на зміст істотної шкоди при вчиненні незаконного втручання.

З урахуванням викладеного можна зробити висновок, що під істотною шкодою при вчиненні незаконного втручання розуміється заподіяння будь-якої шкоди, яку, *виходячи з обставин справи,* може бути

---

[1] [93] Наумов А.В. Применение уголовно-правовых норм. – Волгоград: 1973. – С.97.

[2] [105] Питецкий В. Оценочные понятия в уголовном законе //Советская юстиция. – 1988. – № 12. – С. 7.

[3] [157] Шевченко Є.В. Злочини з похідними наслідками в кримінальному праві: Автореф. дис. … канд. юрид. наук: 12.00.08 /Національна юридична академія України ім. Я. Мудрого. – Х., 2002. – С. 10.

визнано правозастосовником істотною. Зазвичай вона полягає в заподіянні *позитивних матеріальних збитків*. У такому випадку істотну шкоду необхідно оцінювати, виходячи з витрат власника на придбання комп'ютерної інформації. Але іноді вона може виражатися і в *упущеній вигоді*. Це пояснюється тим, що на сучасному етапі будь-яка діяльність як необхідний елемент включає інформаційне забезпечення. Ефективність діяльності багато в чому залежить від кількості та якості вхідної інформації[1], тому перекручення або знищення інформації, що має порівняно невелику ціну, здатне заподіяти значних матеріальних збитків у вигляді упущеної вигоди. Саме тому видається правильним, крім втрати або зменшення обсягу інформації, якою володіє потерпілий, у розмір матеріальних збитків від комп'ютерного злочину включати також і упущену вигоду. При вчиненні незаконного втручання упущена вигода може полягати в укладанні невигідних договорів, падінні авторитету, невиконанні умов договорів тощо.

Для підтвердження обґрунтованості висновку про необхідність включення в розмір істотної шкоди упущеної вигоди варто навести випадок, що мав місце в практиці правоохоронних органів США. Один із співробітників американської компанії, яка працює у сфері високих технологій, був звільнений. Бажаючи помститися адміністрації, він розробив комп'ютерну програму, що через два тижні після звільнення винного знищила комп'ютерну інформацію, що стосувалася новітніх розробок компанії. Збитки від втрачених контрактів і вартість відновлення знищеної інформації становили 10 мільйонів доларів.[2]

---

[1] [122] Семухин И.Ю. Информация – фактор общественного воспроизводства // Матеріали II звітної науково-практичної конференції професорсько-викладацького та курсантського складу Кримського факультету Університету внутрішніх справ. – Сімферополь: Доля, - 2000. – С. 105 – 110.

[2] [161] Former Computer Network Administrator Guilty of Unleashing $10 Million Programming "Timebomb" (May 9, 2000), http://www.usdoj.gov/criminal/cybercrime/njtime.html.

Крім матеріальної шкоди (позитивної та упущеної вигоди), суспільно небезпечні наслідки при вчиненні незаконного втручання можуть виражатися і в *нематеріальних видах шкоди*, що зумовлено розширенням сфери застосування комп'ютерних технологій, використанням ЕОМ, систем та комп'ютерних мереж для контролю складних технологічних процесів, об'єктів і керування ними. Це така шкода, як порушення нормальної роботи підприємств, зупинення або порушення складних технологічних процесів, погіршення обороноздатності держави, підрив авторитету державних органів, підприємств, установ або організацій, створення загрози або заподіяння шкоди життю та здоров'ю громадян, порушення безпеки руху транспорту тощо.

Так, у практиці правоохоронних органів мали місце випадки, коли в результаті незаконного втручання в роботу автоматизованих систем управління порушувався виробничий процес, створювалася загроза життю багатьох осіб (зупинення конвейєра на Волзькому автомобільному заводі[1], збої в роботі автоматизованої системи Ігналінської АЕС[2]). Поширеність комп'ютерних технологій у Збройних силах дозволяє дійти висновку, що одним із можливих наслідків незаконного втручання може бути порушення обороноздатності держави. Наприклад, внаслідок знищення або перекручення комп'ютерної інформації в автоматизованій системі, яка забезпечує управління системами протиповітряної оборони. Знищення або перекручення комп'ютерної інформації в автоматизованих системах, які забезпечують безпеку дорожнього, повітряного або водяного руху, здатне призвести до аварій або катастроф. Незаконне втручання може завдати шкоди авторитету держави, підприємств, установ або організацій. Наприклад, восени 1999 року американський хакер Ерік Барнс у дні, коли

[1] [7] Батурин Ю.М. Компьютерное право: краткий реестр проблем //Советское государство и право. – 1988. – № 8. – С. 63-74

[2] [87] Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления //Законность. – 1997. – № 1. – С. 45.

НАТО бомбило Югославію, перекрутив інформацію, що знаходилася на офіційному сайті Біла Клінтона. Барнс змінив фотографії, які були на сайті, і замінив державний прапор США піратським. Фахівцям президентської адміністрації було потрібно дві доби для того, щоби відновити інформацію, перекручену хакером.[1] Слід відмітити, що визначити вичерпний перелік можливих наслідків незаконного втручання надзвичайно важко, оскільки в кожному випадку ці наслідки залежать, насамперед, від змісту знищуваної або перекручуваної комп'ютерної інформації, який може бути різним.

Таким чином, суспільно небезпечні наслідки при вчиненні незаконного втручання залежать від змісту комп'ютерної інформації, яка знищується або перекручується, і можуть виражатися як у матеріальній шкоді, так і в іншій нематеріальній шкоді, що, як правило, являє собою *більш тяжкі* наслідки, ніж матеріальна. Саме це при дослідженні даного складу порушує питання про відбиття цієї тяжкості в конструкції складу незаконного втручання.

Аналізуючи проблему, не можна не звернути уваги на те, що законодавець у нормах Особливої частини КК по-різному визначає шкоду, заподіювану тим чи іншим злочином: в одних випадках він говорить про істотну шкоду, а в інших – про тяжкі наслідки. При цьому аналіз даних норм дозволяє зробити висновок, що законодавець (у переважній більшості складів) пов'язує істотну шкоду саме з матеріальними збитками. Що ж стосується інших видів шкоди, то здебільшого їх характеризують як тяжкі наслідки. Цей висновок можна підтвердити такою порівняльною таблицею:

Таблиця 1

Статті КК України, які містять кваліфікуючі ознаки у вигляді "тяжких наслідків" і "істотної шкоди"

[1] [55] Кабанников А. Личный хакер Клинтона отправляется в тюрьму //Комсомольская

Статті КК України, Які містять кваліфікуючу (особливо кваліфікуючу) ознаку – "тяжкі наслідки"	**Статті КК України, які містять кваліфікуючу ознаку – "заподіяння шкоди"***
Ст. 110. Посягання на територіальну цілісність і недоторканність України Ст. 133. Зараження венеричною хворобою Ст. 139. Ненадання допомоги хворому медичним працівником Ст. 147. Захоплення заручників Ст. 149. Торгівля людьми або інша незаконна угода щодо передачі людини Ст. 151. Незаконне поміщення в психіатричний заклад Ст. 155. Статеві зносини з особою, яка не досягла статевої зрілості Ст. 161. Порушення рівноправності громадян залежно від їх расової, національної належності або ставлення до релігії Ст. 168. Розголошення таємниці усиновлення (удочеріння) Ст. 188. Викрадення шляхом демонтажу та іншим засобом електричних мереж, кабельних ліній зв'язку та їх обладнання Ст. 236. Порушення правил екологічної безпеки Ст. 241. Забруднення атмосферного повітря Ст. 259. Завідомо неправдиве	Ст. 185. Крадіжка Ст. 186. Грабіж Ст. 189. Вимагання Ст. 192. Заподіяння майнової шкоди шляхом обману або зловживання довірою Ст. 205. Фіктивне підприємництво Ст. 222. Шахрайство з фінансовими ресурсами Ст. 223. Порушення порядку випуску (емісії) та обігу цінних паперів Ст. 224. Виготовлення, збут та використання підроблених недержавних цінних паперів Ст. 289. Незаконне заволодіння транспортним засобом Ст. 410. Викрадення, привласнення, вимагання військовослужбовцем зброї, бойових припасів, вибухових або інших бойових речовин, засобів пересування, військової та спеціальної техніки чи іншого військового майна, а також заволодіння ними шляхом шахрайства або зловживання службовим становищем

правда. – 1999. – 24 ноября. – С. 3.

* У цю колонку не входять статті, що містять кваліфікуючу ознаку "завдання шкоди здоров'ю", оскільки в таких випадках законодавцем дається досить чітка конкретизація шкоди.

повідомлення про загрозу безпеці громадян, знищення чи пошкодження об’єктів власності Ст. 274. Порушення правил ядерної або радіаційної безпеки Ст. 328. Розголошення державної таємниці Ст. 330. Передача або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави Ст. 347. Умисне знищення або пошкодження майна працівника правоохоронного органу	

Аналіз цієї таблиці дозволяє дійти висновку, що, застосовуючи таку кваліфікуючу ознаку, як "істотна чи значна шкода", законодавець пов’язує її з розміром матеріальних збитків. У ряді складів законодавець прямо вказує на це в примітках до статей (наприклад, ст. 185 "Крадіжка"), або, виходячи з аналізу об’єкта й об’єктивної сторони конкретного складу, можна зробити висновок, що істотна шкода виражається саме в матеріальних збитках (наприклад, ст. 222 "Шахрайство з фінансовими ресурсами", ст. 223 "Порушення порядку випуску (емісії) та обігу цінних паперів").

Що ж стосується "тяжких наслідків", то це, як випливає з аналізу, більш широке поняття, що охоплює не тільки заподіяння матеріальних збитків. Про це, крім наведених у таблиці прикладів, свідчить також і те, що в ряді випадків законодавець визнає завдання істотної чи значної шкоди кваліфікуючою ознакою, а настання тяжких наслідків - особливо кваліфікуючою ознакою (наприклад, ст. 424 "Перевищення військовою службовою особою влади чи службових повноважень"). Крім того, у ряді статей (наприклад, ст. 294 "Масові заворушення", ст. 414 "Порушення правил поводження зі зброєю, а також із речовинами і предметами, що становлять підвищену небезпеку для оточення")

законодавець формулює досліджувану ознаку в такий спосіб: "спричинення загибелі людей або настання інших тяжких наслідків". Це також підтверджує висновок про те, що "тяжкі наслідки" – це більш широке поняття, яке містить у собі не тільки завдання матеріальних збитків.

Даний раніше перелік можливих наслідків незаконного втручання дозволяє зробити висновок, що більш обґрунтованою, такою, що точніше відповідає специфіці об’єкта й об’єктивної сторони цього складу злочину, була б така кваліфікуюча ознака, як "настання тяжких наслідків". Тому при подальшому вдосконаленні ст. 361 КК України доцільно було б *виключити з ч. 2 поняття істотної шкоди та доповнити цю статтю частиною третьою*, сформулювавши її таким чином: "дії, передбачені частинами першою чи другою цієї статті, якщо вони спричинили тяжкі наслідки".

Аналізуючи суб’єктивну сторону цього кваліфікованого складу, слід зазначити, що незаконне втручання в роботу ЕОМ, систем або комп’ютерних мереж, яке заподіяло істотну шкоду, належить до злочинів із змішаною формою вини. У таких злочинах психічне ставлення особи до діяння та першого, обов’язкового, наслідку виражається в умислі (прямому або непрямому), а до другого (кваліфікованого) наслідку – тільки в необережності.[1] Отже, вина в досліджуваному злочині виражається в *умисному* вчиненні втручання в роботу ЕОМ, системи або комп’ютерної мережі та умисному знищенні або перекрученні інформації, щодо заподіяння істотної шкоди вина може виражатися тільки в необережності.

4.2. Вчинення незаконного втручання повторно

Повторність обґрунтовано визнається ознакою, що підвищує суспільну небезпечність вчиненого, а тому враховується як обтяжуюча обставина при призначенні покарання (п. 1 ст. 67 КК), а у випадках, передбачених статтями Особливої частини, – як кваліфікуюча ознака. Така ознака міститься і у ст. 361 КК України, ч. 2 якої передбачає відповідальність за незаконне втручання, вчинене повторно.

Відомо, що в науці та практиці поняття повторності тлумачилося неоднозначно, тому, безперечно, позитивним є те, що новий КК України дав визначення цього поняття, встановивши в ч.1 ст. 32, що повторністю злочинів визнається вчинення двох або більше злочинів, передбачених тією самою статтею або частиною статті Особливої частини КК. Таким чином, закон як загальне положення визнає повторністю вчинення тотожних злочинів. Відповідно до цього незаконне втручання слід вважати вчиненим повторно у випадках, коли особа два або більше разів вчинила злочин, який було кваліфіковано за ч. 1 або ч. 2 ст. 361 КК України. При цьому вчинення декількох незаконних втручань не охоплювалося єдиним умислом (злочин не був продовжуваним), особа не звільнялася від кримінальної відповідальності за раніше вчинене незаконне втручання, не закінчилися строки давності притягнення до кримінальної відповідальності за раніше вчинений злочин або судимість за нього не було погашено чи знято.

Аналізуючи загальне поняття повторності, не можна не сказати, що воно значно обмежує можливість урахування підвищеної суспільної небезпечності незаконного втручання, яке вчиняється після однорідного злочину, передбаченого у ст. 362 КК "Викрадення, привласнення, вимагання комп’ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем". Законодавець у ч. 3 ст. 32 КК України передбачає можливість визнання повторним певного злочину за наявності

---

[1] [71] Кримінальне право України: Загальна частина: Підручник для студентів юрид. спец. вищ. закладів освіти /М.І. Бажанов, Ю.В. Баулін, В.І. Борисов та ін.; За ред. професорів М.І.

змішаної повторності, тобто вчинення двох або більше злочинів, передбачених різними статтями КК, якщо таку повторність спеціально передбачено в статтях Особливої частини КК.

Тому визнання незаконного втручання повторним було б доцільним у випадку його вчинення не тільки після такого ж злочину, але й після скоєння злочину, передбаченого ст. 362 КК України. Обґрунтовуючи таку пропозицію, слід зазначити, що, по-перше, ці злочини тотожні за об’єктом і предметом (право власності на інформацію), мають схожу за змістом суб'єктивну сторону, і по-друге, в практиці правоохоронних органів незаконне втручання часто зустрічається разом з незаконним заволодінням комп’ютерною інформацією.

Ураховуючи викладене, статтю 361 КК України доцільно було б доповнити приміткою такого змісту:

" У статтях 361 та 362 повторним визнається злочин, вчинений особою, що раніше вчинила будь-який із злочинів, передбачених цими статтями цього Кодексу.”.

4.3. Вчинення незаконного втручання за попередньою змовою групою осіб

Поняття "вчинення злочину за попередньою змовою групою осіб" до прийняття КК 2001 року в законодавстві України не розкривалося. У науці кримінального права, практиці застосування кримінального закону тлумачення цієї ознаки було неоднозначним, що неґативно позначалося на кваліфікації злочинів, скоєних за попередньою змовою групою осіб.

Пленум Верховного Суду України, а також ряд учених[1] під злочином, вчиненим групою осіб за попередньою змовою, розуміли таке суспільно-

---

Бажанова, В.В. Сташиса, В.Я. Тація. – Київ-Харків: Юрінком Інтер-Право, 2001. – С. 161.

[1] Див.: [75] Кругликов Л.Л., Савинов В.Н. Квалифицирующие обстоятельства: понятие, виды, влияние на квалификацию преступлений: Учебное пособие. – Ярославль: Ярославский университет, 1989. – 86 с.

небезпечне та протиправне діяння, у якому брали участь *співвиконавці,* які заздалегідь (до початку злочину) домовилися між собою про спільне його вчинення. Так, Верховний Суд України, роз'яснюючи правила кваліфікації злочинів за попередньою змовою групою осіб при посяганнях на приватну власність, підкреслив: *"Крадіжку, грабіж, розбій, шахрайство і вимагання слід кваліфікувати як вчинені за попередньою змовою групою осіб тоді, коли за домовленістю, що виникла до початку вчинення відповідного злочину, у ньому брали участь як* ***співвиконавці*** *двоє або більше осіб"*.[1]. Таке розуміння групи осіб за попередньою змовою мало місце і в деяких інших постановах Пленуму Верховного Суду України, наприклад, "Про практику розгляду судами кримінальних справ про виготовлення або збут підроблених грошей або цінних паперів" № 6 від 12 квітня 1996 року[2], "Про судову практику у справах про хабарництво" № 12 від 7 жовтня 1994 року[3], "Про судову практику у справах про злочини проти життя і здоров'я людини" № 1 від 1 квітня 1994 року.[4]

Основним недоліком такого визначення було те, що за межами групи осіб за попередньою змовою, а, отже, у багатьох випадках, за межами кваліфікованих складів злочинів залишалися організатори, підбурювачі, пособники. Це призводило до недооцінки ступеня суспільної небезпечності вчинених злочинів, а також осіб, що їх скоїли, і, урешті-решт, до призначення необґрунтованого покарання.

---

[1] [109] Постанова пленуму Верховного Суду "Про судову практику у справах про корисливі злочини проти приватної власності" № 12 від 25 грудня 1992 року // Збірник постанов Пленуму верховного Суду України кримінальних справах. – Х.: "Одісей", 2000.- С. 135.

[2] [108] Постанова пленуму Верховного Суду "Про практику розгляду судами кримінальних справ про виготовлення або збут підроблених грошей або цінних паперів" від 12 квітня 1996 року № 6 // Збірник постанов Пленуму верховного Суду України кримінальних справах. – Х.: "Одісей", 2000.- С. 157.

[3] [110] Постанова пленуму Верховного Суду "Про судову практику у справах про хабарництво" від 7 жовтня 1994 року № 12 // Збірник постанов Пленуму верховного Суду України кримінальних справах. – Х.: "Одісей", 2000.- С. 227.

[4] [111] Постанова пленуму Верховного Суду України "Про судову практику у справах про злочини проти життя" № 1 від 1 квітня 1994 року // Збірник постанов Пленуму верховного Суду України кримінальних справах. – Х.: "Одісей", 2000.- С. 99 - 100.

КК України 2001 року як загальну норму, що має однакове значення для різних складів злочинів, передбачив саме таку форму співучасті, як "вчинення злочину за попередньою змовою групою осіб", виключивши недоліки, що існували раніше. Як випливає зі змісту ч. 2 ст. 28 КК, “злочин визнається вчиненим за попередньою змовою групою осіб, якщо його спільно вчинили декілька осіб (двоє або більше), які заздалегідь, тобто до початку злочину, домовилися про спільне його вчинення”. Порівнюючи це визначення з поняттям злочину, вчиненого групою осіб без попередньої змови, у якому, відповідно до ч.1 ст. 28, усі співучасники виступають співвиконавцями, можна зробити висновок, що вчинення злочину за попередньою змовою групою осіб законодавець розуміє більш широко: воно буде мати місце не тільки у випадку простої співучасті (співвиконавства) за попередньою змовою, але й у випадках складної співучасті (із розподілом ролей) при наявності такої змови..

Це положення й повинне бути покладене в основу аналізу незаконного втручання, вчиненого групою осіб за попередньою змовою. Специфіка об’єктивної сторони цього складу дозволяє зробити висновок, що він може мати місце в таких випадках:

1) незаконне втручання вчиняється двома або більше виконавцями, кожен з яких виконує всі дії, що утворюють об’єктивну сторону цього складу (наприклад, декілька осіб здійснюють незаконне втручання з окремих терміналів і знищують певну інформцію);
2) незаконне втручання вчиняється двома або більше співвиконавцями, кожен з яких виконує частину дій, що характеризують об’єктивну сторону (наприклад, одна особа вчиняє незаконне втручання й перекручує комп’ютерну інформацію про користувачів комп’ютерної мережі та паролі їх доступу, а друга – знищує комп’ютерну інформацію);
3) незаконне втручання вчиняється двома або більше особами, при цьому лише одна з них виконує роль виконавця, а інші є підбурювачами,

пособниками або організаторами (наприклад, одна особа забезпечує іншу необхідним устаткуванням, а остання вчиняє незаконне втручання, що призводить до перекручення комп'ютерної інформації).

Вимоги до співучасників, передбачені ст. 26 КК, є обов'язковими у всіх випадках: кожен із співвиконавців повинен мати всі ознаки суб'єкта, тобто бути фізичною, осудною особою та досягти віку кримінальної відповідальності. Тому, якщо винний вдається до допомоги завідомо неосудного або малолітнього, то в цьому випадку поставлення за ознаку вчинення злочину за попередньою змовою групою осіб виключається. У випадку, коли особа не була інформована про те, що вчиняє незаконне втручання разом із малолітнім або неосудним, її дії слід кваліфікувати за правилами фактичної помилки як замах на вчинення незаконного втручання в роботу електронно-обчислювальних машин групою осіб за попередньою змовою.

До об’єктивних ознак вчинення злочину за попередньою змовою групою осіб відноситься також спільність, що характеризується взаємозумовленістю дій, загальним для всіх співучасників наслідком і наявністю причинного зв’язку між діями співучасників і злочином, який вчинив виконавець.

Певну специфіку має суб’єктивна сторона незаконного втручання при його вчиненні за попередньою змовою групою осіб. Домовленість про спільне вчинення цього злочину може бути досягнута без особистого знайомства співвиконавців. У практиці російських правоохоронних органів мав місце випадок, коли за допомогою комп’ютерної мережі INTERNET рядом осіб було вчинено розкрадання, причому ці суб’єкти один одного особисто навіть не бачили, оскільки спілкувалися за допомогою електронної мережі, у якій кожен мав свій псевдонім.[1] Подібна співучасть є цілком можливою і при вчиненні незаконного втручання в роботу ЕОМ, систем або комп’ютерних мереж.

[1] [40] Гриднева М. Змей из Интернета //Московский комсомолец. – 1999. – 14 ноября. – С. 7.

На прикладі конкретного злочину проілюструємо можливий розподіл ролей при вчиненні незаконного втручання в роботу ЕОМ. Для одержання контракту на розроблення нового обладнання К., який займається підприємництвом у сфері високих технологій, вирішив знищити комп'ютерну інформацію про нові розробки в комп'ютерній мережі свого конкурента НТП "Атол". Керуючись цією метою, він запропонував своєму заступникові Л. підкупити адміністратора комп'ютерної мережі НТП "Атол" і знайти фахівця з комп'ютерних технологій для знищення інформації в цій комп'ютерній мережі. Виконуючи вказівку К., Л. зустрівся з інженером-програмістом Н., який погодився за винагороду проникнути в комп'ютерну мережу НТП "Атол" і знищити наявну там інформацію. Після цього Л. дістав згоду М., адміністратора комп'ютерної мережі НТП "Атол", за винагороду знищити сліди проникнення Н. у комп'ютерну мережу. У призначений К. день Н. здійснив незаконне втручання в роботу комп'ютерної мережі НТП "Атол" і, знищивши інформацію, сповістив про це К. Останній зв'язався з М., який згідно з домовленістю знищив сліди незаконного втручання Н.

У цій ситуації наявні всі види співучасників, які заздалегідь домовилися про скоєння злочину: К. – організатор, Н. – виконавець, М. – пособник, Л. – підбурювач.

Розділ 5
ВІДМЕЖУВАННЯ НЕЗАКОННОГО ВТРУЧАННЯ В РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН, СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ ВІД СУМІЖНИХ СКЛАДІВ

Правильна правова оцінка вчиненого злочину потребує не тільки співставлення фактичних обставин вчиненого з юридичними ознаками конкретного складу злочину, але й відмежування його від інших, суміжних за деякими ознаками, складів злочинів.[1] Визначення критеріїв відмежування незаконного втручання від суміжних злочинів дозволить глибше проаналізувати зміст його ознак, сприятиме правильній його кваліфікації. Необхідність дослідження питань відмежування незаконного втручання від суміжних злочинів, встановлення критеріїв такого відмежування зумовлена двома обставинами:

1. Незаконне втручання є лише одним із злочинів, об'єднаних загальним родовим об'єктом – інформаційними відносинами у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж, схожих за деякими об'єктивними та суб'єктивними ознаками. Тому правильна кваліфікація незаконного втручання багато в чому визначається чітким відмежуванням його від суміжних комп'ютерних злочинів.

2. Як свідчать результати соціологічних опитувань, на практиці виникають складнощі з розмежуванням незаконного втручання та злочинів, у яких комп'ютерна техніка використовується як знаряддя або засіб вчинення злочину. Тому потребує вирішення питання про відмежування незаконного втручання від ряду злочинів, що посягають на різні об'єкти,

[1] [130] Тарарухин С.А. Квалификация преступлений в следственной и судебной практике. – К.: Юринком, 1995. – С. 80.

але пов’язані з використанням ЕОМ, систем та комп’ютерних мереж як знаряддя або засобу вчинення злочину.

5.1. Відмежування незаконного втручання в роботу електронно-обчислювальних машин, систем та комп’ютерних мереж від інших комп’ютерних злочинів

Відмежування досліджуваного злочину від злочину, передбаченого статтею 362 КК України "Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем", слід проводити за ознаками об’єктивної та суб’єктивної сторін злочину, оскільки безпосередній об’єкт і предмет цих злочинів тотожні.

Виходячи з викладеного в розділі 2 аналізу об’єктивної сторони незаконного втручання, її специфіка виражається в діях, внаслідок яких комп’ютерна інформація, що є предметом злочину, перестає існувати або стає цілком чи частково непридатною для задоволення інформаційної потреби, тобто вона або знищується, або перекручується. При вчиненні злочину, передбаченого ст. 362, комп’ютерна інформація не знищується і не перекручується, нею заволодіває суб’єкт злочину, при цьому вона, як правило, залишається також і у власника комп’ютерної інформації. Така специфіка комп’ютерної інформації як предмета злочину зумовлена можливістю її копіювання. Тому, випадки, коли інформація вилучається у власника, тобто копіюється на носій суб’єкта злочину, а після цього знищується на носії потерпілого, додаткової кваліфікації за ст. 361 КК не потребують, тому що цілком охоплюються ст. 362 КК України.

Із суб’єктивної сторони розмежування між цими злочинами проводиться за видом умислу. Як було вже доведено (розділ 3, підрозділ 3.1), незаконне втручання може вчинятися як з прямим, так і непрямим

умислом. Що стосується викрадення, привласнення, вимагання комп’ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем (ст. 362), то цей злочин вчиняється лише з прямим умислом та корисливим мотивом (винний бажає обернути інформацію на свою користь чи на користь третіх осіб).

Відмежування досліджуваного складу від складу злочину, передбаченого статтею 363 КК – "Порушення правил експлуатації автоматизованих електронно-обчислювальних систем", є більш складним, оскільки стосується практично всіх об’єктивних і суб’єктивних ознак даних складів.

1) Відмежування за об’єктом. Безпосереднім об’єктом незаконного втручання є право власності на комп’ютерну інформацію. Злочин, передбачений ст. 363 КК України, завдає шкоди відносинам щодо забезпечення встановленого порядку експлуатації електронно-обчислювальних машин, їх систем та комп’ютерних мереж.

2) Відмежування за ознаками об’єктивної сторони. Об’єктивна сторона злочину передбаченого статтею 361 КК, як раніше було доведено, полягає в незаконному втручанні, що спричинило знищення чи перекручення комп’ютерної інформації, або в розповсюдженні шкідливих програмних або технічних засобів. Що ж стосується злочину, передбаченого ст. 363 КК України, то його об’єктивна сторона полягає в порушенні правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж, якщо це спричинило викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту або незаконне копіювання комп'ютерної інформації, або істотне порушення роботи таких машин, їх систем чи комп'ютерних мереж.

3) Відмежування за ознаками суб’єктивної сторони. Як вже було сказано, психічне ставлення особи до вчинення незаконного втручання характеризується умислом. Що ж до порушення правил експлуатації ЕОМ,

систем або комп’ютерних мереж, то суб’єктивна сторона цього злочину характеризується змішаною формою вини: стосовно порушення правил експлуатації можливий як умисел, так і необережність, а відносно наслідків (викрадення, перекручення чи знищення комп’ютерної інформації, засобів її захисту, незаконне копіювання комп’ютерної інформації, істотне порушення роботи ЕОМ, їх систем чи комп’ютерних мереж) – тільки необережність.[1] Якщо особа умисно порушує правила експлуатації і її умислом (прямим або непрямим) охоплюється настання зазначених наслідків, то такі дії слід розцінювати як незаконне втручання (ст. 361 КК України) або як викрадення, привласнення, вимагання комп'ютерної інформації або (відповідно за метою) заволодіння нею шляхом шахрайства чи зловживання службовим становищем (ст. 362 КК України).

4) Відмежування за ознаками суб’єкта. Обов’язковою ознакою порушення правил експлуатації автоматизованих електронно-обчислювальних машин є спеціальний суб’єкт – особа, яка відповідає за їх експлуатацію. Суб’єкт незаконного втручання – загальний.

5.2. Відмежування незаконного втручання від злочинів, пов’язаних із використанням комп’ютерної техніки як знаряддя або засобу вчинення злочину

1. Виходячи з того, що безпосереднім об’єктом незаконного втручання є право власності на комп’ютерну інформацію, із необхідністю виникає проблема відмежування його від злочинів проти власності, передбачених *главою VI КК України.*

[1] [72] Кримінальне право України: Особлива частина: Підручник для студентів юрид. спец. вищ. закладів освіти /М.І. Бажанов, В.Я. Тацій, В.В. Сташис, І.О. Зінченко та ін.; За ред. професорів М.І. Бажанова, В.В. Сташиса, В.Я. Тація. – Київ-Харків: Юрінком Інтер-Право, 2001. – С. 390.

За об’єктивною стороною незаконне втручання подібне до такого злочину проти власності, як умисне знищення або пошкодження майна: і в тому, і в іншому складі діяння виражається в активній поведінці, яка спричиняє повну або часткову непридатність предмета злочину для використання за цільовим призначенням. Наслідки в цих складах також подібні. І в першому, і в другому власник предмета або істотно обмежується у своїх правах, або цілком втрачає можливість реалізувати своє право власності на предмет, і, як правильно зазначається в літературі, подальше його використання за функціональним призначенням можливе "лише за необхідних фінансових, трудових та інших витрат".[1]

Тому основні відмінності даних складів слід шукати в ознаках об’єкта та предмета посягань. Відповідно до закону безпосереднім об’єктом умисного знищення або пошкодження майна (ст. 194 КК) є право власності на річ. Безпосереднім же об’єктом незаконного втручання, як випливає з закону і було аргументовано в розділі 1 цієї роботи, є право власності на інформацію. Відмінність даних суспільних відносин полягає в тому, що перші – це форма реалізації соціального інтересу щодо володіння, користування та розпоряджання *майном*, а другі – щодо *інформації*. Відмінність між інформацією і річчю полягає, насамперед, у їх фізичній властивості. Майно є об’єктом матеріального світу. Що ж стосується інформації, то вона, як зазначалося в розділі 1, не може бути віднесена ні до матеріальних, ні до нематеріальних об’єктів: фізична властивість інформації полягає в наявності матеріального носія, але йому вона не тотожна.

Відмінність ознак об’єкта та предмета зумовлює і різний зміст ознак об’єктивної сторони незаконного втручання та умисного знищення або пошкодження майна. Знищення або пошкодження майна полягає в порушенні, як правило, його фізичної цілісності, а знищення або

[1] [72] Там само. – С. 150.

перекручення комп'ютерної інформації не завжди супроводжується порушенням цілісності її носія.

Визначаючи критерії відмежування незаконного втручання від інших злочинів проти власності, необхідно відмітити, що досить часто при вчиненні посягань на відносини власності комп'ютерна техніка виступає в ролі предмета або засобу злочину. Видається можливим виділити три варіанти кваліфікації таких випадків.

По-перше, комп'ютерна техніка може використовуватися для вчинення розкрадань. Такі злочини неодноразово зустрічалися в практиці правоохоронних органів України. Так, у 1995 році в Дніпропетровському регіональному управлінні Промінвестбанку України було викрадено близько 864 млн. крб. Роком пізніше у відділенні АКБ "Україна" у м. Сімферополі з використанням комп'ютерної техніки було викрадено близько 450 млн. крб.[1], а у 1994 році в Черкаській обласній дирекції Укрсоцбанку вчинено розкрадання 990 млн. крб.[2] Правоохоронні органи України в 1996 році запобігли спробам незаконного переказу з рахунку Національного банку України в АКБ "Таврія" 10 млн. гривень, спробам втручання в електронну систему Мелітопольского відділення АК АПБ "Україна" із метою крадіжки 448 тис. гривень, а також спробам крадіжки 182 тис. гривень із використанням електронних міжбанківських розрахунків у Закарпатському відділенні банку "Аваль".[3] Восени 1998 року з використанням комп'ютерної системи електронних платежів близько 80

---

[1] [31] Гавриленко І. Комп'ютерна злочинність // Юридичний вісник України. – 1997. – № 28 – С. 3.

[2] [27] Волобуєв А.Ф. Особливості розслідування розкрадань грошових коштів, що здійснюються з використанням комп'ютерної техніки //Вісник Луганського інституту внутрішніх справ. – 1998. – № 2. – С. 97.

[3] [30] Гавловський В.Д., Цимбалюк В.С. Щодо проблем боротьби із злочинами, що вчинюються з використанням комп'ютерних технологій //Уряду України. Президенту, законодавчій, виконавчій владі "Боротьба з контрабандою: проблеми та шляхи їх вирішення". Аналітичні розробки, пропозиції наукових і практичних працівників /Керівники авторського колективу А.І. Комарова, О.О. Крикун. – К., 1998. – С. 148-154.

млн. гривень було викрадено з рахунків Вінницької дирекції НБУ.[1] Механізм учинення таких злочинів, як правило, полягає в тому, що електронна система переказу платежів, яка використовується тією чи іншою фінансовою установою, застосовується злочинцем для здійснення незаконного переказу коштів. Наприклад, у вересні 1997 року в Луганському відділенні АКБ "Укркомунбанк" бухгалтер операційного відділу використала комп'ютерну систему банку для викрадення 300 тис. гривень. Отримавши меморіальний ордер, вона ввела в систему реквізити не одержувача за даним ордером, а іншої організації, однак довести свій умисел до кінця не змогла, оскільки спрацювала система захисту. За цим фактом Ленінським РВ ЛМУ УМВС України в Луганській області було порушено кримінальну справу: дії бухгалтера правильно кваліфіковано як замах на розкрадання колективного майна в особливо крупних розмірах. Ознаки незаконного втручання в таких діях відсутні, оскільки винний, віддаючи команду комп'ютерній системі переказу платежів, не перекручує і не знищує комп'ютерну інформацію, яка зберігається в ній. Слід зазначити, що в новому КК міститься спеціальна норма для кваліфікації таких дій. Частина 3 статті 190 передбачає кримінальну відповідальність за шахрайство, вчинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки.

На особливу увагу заслуговують випадки, які у світовій практиці одержали назву "крадіжка машинного часу". Такого роду злочини полягають у тому, що особа неправомірно використовує дороге комп'ютерне устаткування (наприклад, суперкомп'ютери) або ресурси комп'ютерних мереж, *абонентом яких вона не є*. В Україні один із перших таких злочинів було скоєно в Чернігові. У вересні 1998 року більше 10 клієнтів ЗАТ "Сінет", яке надає послуги INTERNET, одержали до оплати

[1] [29] Воры проникли в компьютерную сеть Национального банка //Голос Украины. – 1998. – № 217 (1963). – 5 ноября. – С. 3.

явно завищені рахунки. Більшість із цих клієнтів були організаціями, а в рахунках указувалося, що під їх ім’ям неодноразово здійснювалася робота в INTERNET переважно з 1 до 4 години. Правоохоронними органами було встановлено, що група осіб одержала інформацію про імена абонентів комп’ютерної мережі INTERNET та їхні паролі доступу. Після цього, застосовуючи стандартне устаткування та програмне забезпечення для віддаленого доступу, ці особи використовували ресурси мережі INTERNET від чужого імені, чим завдали матеріальних збитків провайдеру (ЗАТ "Сінет") і ряду його клієнтів. За цим фактом прокуратурою Чернігова у травні 1999 року було порушено кримінальну справу. Дії осіб, які вчинили "крадіжку машинного часу", були неправильно кваліфіковані як незаконне втручання в роботу автоматизованих систем (стаття 198^1 КК 1960 року), тому районним судом було прийнято рішення про повернення справи на додаткове розслідування. Прокуратурою це рішення було опротестовано, однак в апеляційному суді протест не задовольнили. Слід зазначити, що в цьому випадку об’єктом посягання не були відносини інформаційної діяльності у сфері застосування ЕОМ, їх систем або комп’ютерних мереж. Указані дії заподіювали шкоду відносинам власності потерпілих. Провайдеру та його клієнтам належать оплачувані ними послуги користування INTERNET, а особи, які вчинили "крадіжку машинного часу", неправомірно використовували ці ресурси. У зв’язку з цим рішення, прийняті районним та апеляційним судами, слід визнати правильними, а правильною кваліфікацією подібних дій, як видається, є їх оцінка як заподіяння майнової шкоди шляхом обману або зловживання довірою (стаття 192 КК України). Ознаки незаконного втручання в даному випадку відсутні, оскільки робота в INTERNET передбачає ознайомлення з різного роду відкритою інформацією, при цьому інформація, яка знаходиться в INTERNET, не знищується і не перекручується.

По-друге, незаконне втручання може бути способом вчинення злочину проти власності. У цих випадках такі дії необхідно кваліфікувати за двома статтями: статтею, що передбачає відповідальність за злочин проти власності, і статтею, що передбачає відповідальність за незаконне втручання. Фахівцями відзначається значне поширення розкрадань матеріальних і фінансових коштів шляхом перекручення змісту комп'ютерної інформації.[1] Прикладом таких дій є випадок, який наводився у розділі 3, де головний інженер-електронник Центру інформаційних технологій і технічного забезпечення Донецької дирекції Українського Державного підприємства електрозв'язку "Укртелеком" заподіяв збитки цьому підприємству в розмірі близько 150 тисяч гривень. Ці дії були правильно кваліфіковані як сукупність злочинів, передбачених статтями 86^1 і 198^1 КК України 1960 року. Основним об'єктом посягання у наведеному випадку виступають відносини власності, а додатковим – відносини інформаційної діяльності у сфері використання електронно-обчислювальної техніки. Схожий випадок мав місце влітку 2002 року в Херсоні. Студент одного з вузів міста вчинив незаконне втручання в роботу комп'ютерної мережі місцевого провайдера інтернет-послуг і перекрутив комп'ютерну інформацію про рахунки клієнтів та сплачений час роботи в мережі Інтернет (створив фіктивний рахунок). Після цього протягом кількох місяців безкоштовно користувався Інтернетом, чим заподіяв матеріальну шкоду провайдерові у розмірі 11000 грн.[2] За чинним КК подібні дії необхідно кваліфікувати як сукупність злочинів, передбачених статтями 185, 190, 191 або 192 і статтею 361. Саме так слід робити і у випадках вчинення

[1] [98] Овчинский В.С. XXI век против мафии. Криминальная глобализация и Конвенция ООН против транснациональной организованной преступности. – М.: ИНФРА-М, 2001. – С. 22-23.

[2] [119] Свиридов С. "Капкан" для хакера // Комсомольская правда. – 2002. – 10 сентября. – С. 5.

вимагання, поєднаного зі знищенням або перекрученням комп'ютерної інформації.

По-третє, злочин проти власності, предметом якого є комп'ютерна техніка, може виступати як спосіб вчинення незаконного втручання. Розкрадання та пошкодження комп'ютерної техніки – це звичайні злочини проти власності, тому труднощів із кваліфікацією таких дій не виникає. Від незаконного втручання вони відрізняються за об'єктом (право власності на річ і право власності на комп'ютерну інформацію), предметом (комп'ютерна техніка і комп'ютерна інформація), об'єктивною стороною (розкрадання, пошкодження, знищення техніки та знищення, перекручення комп'ютерної інформації). Однак найголовнішою ознакою відмежування злочинів проти власності від незаконного втручання є спрямованість умислу. Якщо дії особи являють собою порушення фізичної цілісності комп'ютерної техніки (ознака об'єктивної сторони злочину проти власності), але мета, яку переслідує суб'єкт, полягає в заподіянні шкоди відносинам власності на інформацію, то дії цієї особи слід кваліфікувати як незаконне втручання в роботу ЕОМ, систем та комп'ютерних мереж, оскільки знищення або пошкодження комп'ютерної техніки в цьому випадку є способом вчинення незаконного втручання в роботу ЕОМ, систем або комп'ютерних мереж. Кваліфікувати подібні дії необхідно як сукупність злочинів, передбачених статтею 361 "Незаконне втручання в роботу електронно-обчислювальних машин" і статтею 194 "Умисне знищення або пошкодження майна".

2. Важливим питанням у визначенні критеріїв відмежування незаконного втручання від суміжних злочинів є визначення ознак, які дозволяють розмежувати незаконне втручання і злочин, передбачений *ст. 357 КК України* "Крадіжка, присвоєння, вимагання документів, штампів, печаток, заволодіння ними шляхом шахрайства або зловживання службовим становищем або їх пошкодження". Оскільки документ є одним

із видів інформації, подібність зазначених складів полягає в тому, що ст. 357 і ст. 361 КК України передбачають відповідальність за знищення або перекручення інформації. Розмежовувати незаконне втручання та пошкодження або знищення документів необхідно за ознаками предмета злочину.

Документ являє собою передбачену законом матеріальну форму одержання, зберігання, використання та розповсюдження інформації, зафіксованої на папері, магнітній, кіно-, відео- та фотоплівці, оптичному диску або іншому носії. Предметом злочину, передбаченого ст. 357 КК України, є документи, які підтверджують факти, що мають юридичне значення. Саме за цією ознакою слід розмежовувати злочин, передбачений ст. 357 КК України, і незаконне втручання: якщо певна комп'ютерна інформація є передбаченою законом формою фіксації відомостей, що підтверджують факти, які мають юридичне значення, то її знищення або пошкодження, за відповідних ознак суб'єктивної сторони злочину, необхідно кваліфікувати не за ст. 361, а за ст. 357 КК України.

3. На окрему увагу заслуговує питання відмежування незаконного втручання від злочинів проти встановленого порядку обігу таємної інформації та відомостей, що становлять комерційну таємницю або таємницю приватного життя. Одержання за допомогою комп'ютерної техніки таких відомостей є злочином, передбаченим статтями 111, 114, 231 або 182 КК України. Основною ознакою відмежування цих злочинів є об'єктивна сторона. У незаконному втручанні вона полягає у знищенні чи перекрученні інформації, а в перелічених вище злочинах – у незаконному одержанні інформації. Специфічна і суб'єктивна сторона цих злочинів: її обов'язковою ознакою є мета – використання такої інформації. У разі відсутності такої мети вчинене, за наявності відповідних ознак, необхідно кваліфікувати як незаконне втручання або як викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом

шахрайства чи зловживання службовим становищем (ст. 362 КК України). Слід зазначити, що у практиці зарубіжних правоохоронних органів зустрічалися випадки посягання на закриту комп'ютерну інформацію без мети її використання. Наприклад, у лютому 1998 року громадянин Ізраїлю Ехуд Тенебаум здійснив незаконне втручання в роботу комп'ютерів Міністерства оборони США, де зберігалася закрита інформація. У процесі розслідування було встановлено, що мотив і мета зловмисника не дозволяють кваліфікувати його дії як шпигунство.[1] Як би ці події відбувалися на території України, то дії ізраїльського громадянина треба було б кваліфікувати як незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж.

4. У питанні відмежування замаху на незаконне втручання від суміжних злочинів у разі, коли відсутні наслідки незаконного втручання у вигляді знищення або перекручення комп'ютерної інформації, можна погодитися з П.П. Андрушком. Він зазначає, що залежно від мети такого втручання його можна кваліфікувати: за ст. 114 або ст. 231 (за наявності ознак цих злочинів), якщо метою втручання в роботу ЕОМ, їх систем чи комп'ютерних мереж було незаконне ознайомлення з інформацією, яка в них опрацьовується чи зберігається; за іншими статтями КК, що передбачають відповідальність за злочини, спосіб вчинення яких може виражатися в незаконному втручанні, наприклад: розкрадання майна, виготовлення з метою збуту чи використання підроблених недержавних цінних паперів (ст. 224) або незаконні дії з документами на переказ та іншими засобами доступу до банківських рахунків (ст. 200).[2]

---

[1] [163] Israeli Citizen Arrested in Israel for Hacking United States and Israeli Government Computers (March 18, 1998), http://usdoj.gov/criminal/cybercrime/ehudpr.html

[2] [90] Науково-практичний коментар до Кримінального кодексу України. За станом законодавства і постанов Пленуму Верховного Суду України на 1 грудня 2001 р./ За ред. С.С. Яценка. – К.: А.С.К., 2002. – С. 783-787.

5. Незаконне втручання слід відмежовувати й від порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються через комп'ютер (ст. 163 КК України). Незаконне отримання кореспонденції, що передається з використанням засобів електронної пошти не відноситься до комп'ютерних злочинів, а являє собою злочин проти особистих прав та свобод людини. Від комп'ютерних злочинів цей склад відрізняється за предметом: предмет комп'ютерних злочинів – комп'ютерна інформація, предмет злочину, передбаченого ст. 163 КК України, специфічний вид інформації - кореспонденція; а також за об'єктом посягання: право власності на комп'ютерну інформацію та недоторканність приватного життя.

6. Комп'ютерна технологія призвела до появи нових об'єктів інтелектуальної власності: програмного забезпечення та топографій інтегральних мікросхем, які стали новими видами предметів злочинів проти інтелектуальної власності (ст. ст. 176, 177 КК України). Отже, необхідним є відмежування незаконного втручання від цих злочинів. Різниця даних злочинів полягає в ознаках об'єкта, предмета та об'єктивної сторони. Безпосередніми об'єктами злочину, передбаченого ст. 176 КК, виступають авторські права (особисті немайнові та майнові права авторів, їх правонаступників, пов'язані зі *створенням* та використанням творів науки, літератури, мистецтва) і суміжні права (права виконавців, виробників фонограм, організаторів мовлення, пов'язані з використанням творів). Безпосередній об'єкт порушення прав на об'єкти промислової власності (ст 177 КК) складають відносини володіння, розпоряджання, користування результатом *своєї творчості* в будь-якій сфері промисловості чи господарської діяльності.[1] Ці норми *охороняють інтереси автора*, особи

[1] [71] Кримінальне право України: Особлива частина: Підручник для студентів юрид. спец. вищ. закладів освіти /М.І. Бажанов, В.Я. Тацій, В.В. Сташис, І.О. Зінченко та ін.; За ред. професорів М.І. Бажанова, В.В. Сташиса, В.Я. Тація. – Київ-Харків: Юрінком Інтер-Право, 2001. – С. 104 – 107.

яка створила певні об’єкти інтелектуальної власності. У свою чергу, незаконне втручання являє собою посягання на суспільні відносини іншого змісту - відносини володіння, користування та розпоряджання комп’ютерною інформацією, як її авторів, так і осіб, котрі такими не є.

З цього положення випливає другий критерій, який дозволяє розмежувати незаконне втручання в роботу електронно-обчислювальних машин, систем та комп’ютерних мереж від порушення авторського права, а саме - предмет посягання. Предметом першого з вказаних злочинів є комп’ютерна інформація, предметом останнього – тільки об’єкти авторського права, до яких діюче законодавство України відносить, зокрема, програми для електронно-обчислювальних машин та бази даних.

Слід також відзначити, що потерпілим від незаконного втручання може бути будь-яка фізична чи юридична особа або держава якщо їй належить право власності на комп’ютерну інформацію, а потерпілим від порушення авторського права та суміжних прав визнається тільки автор того чи іншого об’єкта авторського права або особа, якій на законних підставах належить виключне чи невиключне авторське право.

Різниця між безпосередніми об’єктами зумовлює й різний зміст об’єктивної сторони цих злочинів. Порушення авторських чи суміжних прав полягає у незаконному використанні об’єктів авторського права (наприклад, розповсюдження програми для ЕОМ або перекручення відомостей про автора програми). При вчиненні незаконного втручання подальше використання винним комп’ютерної інформації, що була знищена чи перекручена не є обов’язковим.

Таким чином, слід зазначити, що комп’ютерна техніка може використовуватися для вчинення багатьох злочинів, однак використання комп’ютерної техніки ще не дозволяє говорити про те, що скоєно комп’ютерний злочин. Основним критерієм відмежування незаконного втручання і взагалі комп’ютерних злочинів від злочинів, пов’язаних із

використанням комп’ютерної техніки як знаряддя або засобу є об’єкт злочину.

ВИСНОВКИ

Відповідно до мети та завдань даного дослідження визначені юридичні ознаки складу злочину "Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем чи комп'ютерних мереж", передбаченого ст. 361 КК України.

1. На основі аналізу змін у суспільних відносинах на сучасному етапі, викликаних появою та розширенням сфери застосування комп'ютерної техніки, аналізу факторів суспільної небезпечності злочинів у сфері використання електронно-обчислювальних машин, систем і комп'ютерних мереж, а також висловлених у науці позицій з цього питання пропонується таке визначення *родового об'єкта* незаконного втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж: інформаційні відносини у сфері використання електронно-обчислювальних машин, систем або комп'ютерних мереж.

2. Обґрунтовується необхідність введення такого терміна, як *"комп'ютерний злочин"* стосовно до злочинів, передбачених у розділі XVI КК України. Проаналізувавши наявні в науці кримінального права визначення комп'ютерних злочинів, пропонується таке їх визначення: комп'ютерні злочини – суспільно небезпечні, винні, кримінально карані, діяння, що завдають шкоди інформаційним відносинам, засобом забезпечення яких є електронно-обчислювальні машини, системи або комп'ютерні мережі.

3. *Безпосередній об'єкт* аналізованого злочину визначається як охоронювана кримінальним законом структурно організована й нормативно врегульована система соціально значущих *відносин власності на комп'ютерну інформацію*, яка забезпечує свободу реалізації права кожного учасника на задоволення інформаційної потреби.

4. Ознаки, що характеризують *комп'ютерну інформацію як предмет злочину*, співвідносяться з ознаками предмета злочину проти власності. Це видається найбільш вдалим, оскільки злочини проти власності – "генетично" найближча до незаконного втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж група злочинів. Фізичною ознакою комп'ютерної інформації як предмета злочину є наявність носія – предмета чи сигнала, фізичні, хімічні чи інші властивості яких використовуються для зберігання або передачі інформації, розпізнаваної електронно-обчислювальною машиною. Економічна ознака комп'ютерної інформації як предмета злочину виражається в тому, що вона є цілісною, конфіденційною, має ціну. Юридична ознака комп'ютерної інформації виражається в тому, що вона є чужою для винного і має власника. Виходячи з викладеного, *комп'ютерна інформація як предмет злочину* визначається таким чином: відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника і ціну.

5. На основі цього положення обґрунтовується недоцільність законодавчого визначення носія інформації як самостійного предмета незаконного втручання. Оскільки, по-перше, носій інформації є фізичною ознакою комп'ютерної інформації, отже, по-друге, поняттям "знищення або перекручення комп'ютерної інформації" повністю охоплюється поняття "знищення або перекручення носія комп'ютерної інформації".

6. Досліджуючи зміст поняття "комп'ютерний вірус", відзначається, що:

1) незважаючи на безліч різних підходів до визначення комп'ютерного вірусу, чіткої його дефініції досі немає;

2) комп'ютерний вірус являє собою комп'ютерну програму, спеціально призначену для знищення або перекручення комп'ютерної

інформації, інакше кажучи, по своїй суті він є одним з видів програмних засобів, призначених для незаконного проникнення в електронно-обчислювальні машини, системи чи комп'ютерні мережі та здатних спричинити перекручення або знищення інформації.

На основі цього робиться висновок про недоцільність виділення в диспозиції статті 361 КК комп'ютерного вірусу як самостійного предмета незаконного втручання. На думку дисертанта, більш правильною була б така характеристика предмета аналізованого злочину: програмні й технічні засоби, призначені для незаконного проникнення в електронно-обчислювальні машини, системи чи комп'ютерні мережі та здатні спричинити перекручення або знищення інформації (шкідливі програмні й технічні засоби).

Програмні засоби, спеціально призначені для незаконного втручання в роботу ЕОМ, систем, комп'ютерних мереж, – це програми (програмні блоки, програмне забезпечення), розроблені спеціально для несанкціонованого доступу до комп'ютерної інформації, для перекручення, знищення, незаконного копіювання такої інформації або вчинення інших порушень права власності на неї.

Технічні засоби, спеціально призначені для порушення права власності на комп'ютерну інформацію, – це різного роду пристрої, обладнання, спеціально розроблені для отримання незаконного доступу до комп'ютерної інформації, її знищення або перекручення, іншого порушення права власності на неї.

7. Аналіз диспозиції статті 361 КК дає можливість зробити висновок про те, що незаконне втручання можливе у двох різних формах:

1) незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж, яке спричинило перекручення або знищення комп'ютерної інформації чи носіїв такої інформації;

2) розповсюдження комп’ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані електронно-обчислювальні машини, їх системи чи комп’ютерні мережі та здатних спричинити перекручення або знищення комп’ютерної інформації чи носіїв такої інформації.

Виходячи з законодавчої конструкції, перша з цих форм незаконного втручання є злочином із матеріальним складом, тобто обов’язковими ознаками його об’єктивної сторони в даному випадку є діяння, наслідок і причинний зв’язок.

Діяння в цій формі виражається в незаконному втручанні в роботу електронно-обчислювальних машин, систем, комп’ютерних мереж, яке визначається таким чином: зміна шляхом впливу на носій інформації режиму їх роботи, яка порушує встановлений нормативно-правовими актами порядок використання ЕОМ, систем чи комп’ютерних мереж. Така зміна ставить під загрозу функціонування ЕОМ у плані зберігання, опрацювання, зміни або доповнення і тим самим порушує суспільні відносини, які забезпечують застосування автоматизованих систем для поліпшення певної діяльності людини, а також відносини передачі й отримання інформації з застосуванням комп’ютерних мереж.

Різні способи незаконного втручання в роботу ЕОМ, систем, комп’ютерних мереж, виходячи з характеристики засобів, які застосовуються для вчинення незаконного втручання, класифікуються: на способи, що ґрунтуються на використанні засобів спеціального технічного впливу; способи, що ґрунтуються на використанні програмного забезпечення; змішані способи. Серед багатьох способів деяку специфіку має лише один, для позначення якого вживається термін "несанкціонований доступ". Він визначається таким чином: спосіб вчинення незаконного втручання в роботу ЕОМ, систем, комп’ютерних мереж, який полягає в отриманні можливості здійснювати різні дії з комп’ютерної інформацією,

що має специфічні технічні чи програмні засоби захисту від її знищення або перекручення. На основі аналізу практики боротьби з комп'ютерними злочинами та зарубіжного кримінального законодавства зроблено висновок про підвищену суспільну небезпечність такого способу вчинення незаконного втручання. Це й визначає доцільність виділення несанкціонованого доступу як кваліфікуючої ознаки складу незаконного втручання. Тому пропонується доповнити ч. 2 ст. 361 КК України вказівкою на цю ознаку: "Ті самі дії … вчинені шляхом несанкціонованого доступу до комп'ютерної інформації".

Диспозиція статті 361 КК України в якості обов'язкового наслідку незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж передбачає знищення або перекручення комп'ютерної інформації, поняття яких розкриваються таким чином:

знищення комп'ютерної інформації – це такий вплив на носій комп'ютерної інформації, внаслідок якого вона перестає існувати у формі, що дозволяє її опрацювання за допомогою комп'ютерної техніки, стає непридатною для задоволення інформаційної потреби особою, яка має право власності на таку інформацію;

перекручення комп'ютерної інформації – це такий вплив на носій комп'ютерної інформації, який полягає в зміні без відома власника змісту відомостей, відбитих на носії, що робить інформацію повністю, частково або тимчасово непридатною для задоволення інформаційної потреби власником інформації.

Причинний зв'язок як обов'язкова ознака об'єктивної сторони першої форми незаконного втручання характеризується тим, що він є проявом закономірного зв'язку між діяння і наслідками і виступає необхідною умовою, без якої наслідки у вигляді знищення або перекручення інформації не настали б. Відсутність необхідного причинного зв'язку виключає об'єктивну сторону незаконного втручання в

роботу електронно-обчислювальних машин, систем і комп'ютерних мереж. Закінченим незаконне втручання в цій формі буде з моменту настання суспільно небезпечних наслідків у вигляді знищення або перекручення інформації за умови відсутності її копій на інших носіях комп'ютерної інформації.

Другу форму об'єктивної сторони незаконного втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж законодавець конструює як злочин з формальним складом. Незаконне втручання в цій формі вважається закінченим з моменту вчинення самого діяння: розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані електронно-обчислювальні машини, їх системи чи комп'ютерні мережі та здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації.

Проведений аналіз змісту поняття "розповсюдження комп'ютерного вірусу способом застосування програмних і технічних засобів" дозволив дійти висновку, що диспозиція статті 361 не охоплює повною мірою всі можливі способи вчинення цього злочину, які відомі в інформатиці й трапляються в практиці. Крім того, неточність законодавчого визначення виявляється і в тому, що комп'ютерний вірус самий по собі є одним із шкідливих програмних засобів. У зв'язку з цим пропонується нова редакція диспозиції ст. 361 КК у частині визначення другої форми об'єктивної сторони незаконного втручання:

"розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в ЕОМ, системи чи комп'ютерні мережі та здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації".

З урахуванням запропонованої редакції об'єктивна сторона в даній формі порушення роботи ЕОМ, систем чи комп'ютерних мереж полягала б:

по-перше, у розповсюдженні шкідливих програмних засобів, тобто в оплатній або безоплатній передачі шкідливого програмного забезпечення, а також його копіюванні, самовідтворенні, встановленні в програмне забезпечення або його розповсюдженні з допомогою комп'ютерних мереж; по-друге, у розповсюдженні шкідливих технічних засобів, тобто в їх оплатній або безоплатній передачі, а також їх встановленні в ЕОМ, системи чи комп'ютерні мережі.

8. Аналізуючи зміст умислу при незаконному втручанні автор вважає, що, усвідомлення особою фактичних ознак вчинюваного злочину полягає в розумінні винним *у загальних рисах закономірностей* функціонування ЕОМ: не потрібно, щоб винний охоплював свідомістю всі деталі складного процесу функціонування ЕОМ.

Як необхідна ознака умислу в аналізованому складі виступає *усвідомлення протиправності*: вчиняючи втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж, суб'єкт злочину усвідомлює відсутність у нього права на знищення або перекручення комп'ютерної інформації, а отже, незаконність порушення ним встановленого власником інформації порядку використання електронно-обчислювальних машин, систем і комп'ютерних мереж.

Передбачення можливості чи неминучості перекручення або знищення комп'ютерної інформації припускає чітке уявлення винним розвитку причинного зв'язку між незаконним втручанням і перекрученням або знищенням комп'ютерної інформації. Особа, яка вчинює аналізований злочин, передбачає, що саме в результаті вчинюваних нею дій інформація буде знищена чи перекручена і можливість власника інформації здійснювати свої повноваження буде виключена або значно погіршена.

Вольовий момент умислу при вчиненні незаконного втручання полягає в бажанні чи свідомому допущенні перекручення або знищення комп'ютерної інформації. Про його наявність і зміст можуть свідчити

характер дій, спосіб вчинення незаконного втручання, мотиви й цілі, якими керується особа.

Для наявності вини в другій формі - розповсюдженні шкідливих програмних чи технічних засобів - достатньо усвідомлення особою суспільної небезпечності розповсюдження шкідливих програмних чи технічних засобів, незаконності таких дій, а також розуміння того, що розповсюджувані засоби спеціально призначені для незаконного втручання в роботу електронно-обчислювальних машин, тобто є шкідливими. У разі, якщо особа не усвідомлює таких властивостей програмних чи технічних засобів, які нею розповсюджуються, кримінальна відповідальність за розповсюдження шкідливих засобів виключається.

9. Суб'єктом незаконного втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж є фізична осудна особа, яка досягла 16-ти років.

10. Аргументується висновок про необхідність визначення ознак спеціального суб'єкта незаконного втручання та пропонується доповнити ч. 2 ст. 361 КК України кваліфікуючою ознакою: вчинення незаконного втручання особою, яка має доступ до ЕОМ, системи чи комп'ютерної мережі у зв'язку з займаною посадою або спеціальними повноваженнями.

11. На основі аналізу змісту поняття істотної шкоди як кваліфікуючої ознаки незаконного втручання робиться висновок про те, що суспільно небезпечні наслідки при вчиненні незаконного втручання полягають не тільки в знищенні або перекрученні комп'ютерної інформації, а можуть виражатися як у заподіянні матеріальної шкоди (позитивної чи упущеної вигоди), так і в іншій, нематеріальній шкоді, що, як правило, являє собою більш тяжкі наслідки, ніж матеріальна шкода. Між тим, з аналізу норм Особливої частини КК випливає, що законодавець (у переважній більшості складів) пов'язує істотну шкоду саме тільки з матеріальною шкодою. Це дозволяє зробити висновок, що більш обґрунтованою, більш відповідною до

специфіки об’єкта й об’єктивної сторони цього складу була б така кваліфікуюча ознака, як "настання тяжких наслідків". Тому, удосконалюючи ст. 361 КК України, доцільно виключити з ч. 2 поняття "істотна шкода" та доповнити цю статтю частиною 3, сформулювавши її таким чином: " Дії, передбачені частинами першою чи другою цієї статті, якщо вони спричинили тяжкі наслідки ".

12. Робиться висновок, що більш доцільним було б визнання незаконного втручання повторним у разі його вчинення не тільки після вчинення тотожного злочину, а й після вчинення злочину, передбаченого ст. 362 КК України "Викрадення, привласнення, вимагання комп’ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем", і пропонується доповнити ст. 361 КК України приміткою такого змісту:

" У статтях 361 та 362 повторним визнається злочин, вчинений особою, що раніше вчинила будь-який із злочинів, передбачених цими статтями цього Кодексу.".

13. Визначаються ознаки, які дозволяють відмежувати незаконне втручання від двох суміжних груп злочинів: по-перше, від інших злочинів, передбачених розділом XVI КК, а по-друге, від злочинів проти власності, передбачених розділом VI Особливої частини КК України та рядом інших статей КК.

Виходячи з викладеного пропонується нова редакція статті 361 КК України "Незаконне втручання в роботу електронно-обчислювальних машин, систем та комп’ютерних мереж":

1. Незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж, що призвело до перекручення чи знищення комп'ютерної інформації, а також розповсюдження 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, -

караються штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на той самий строк.

2. Ті самі дії, вчинені повторно чи за попередньою змовою групою осіб або особою, яка має доступ до електронно-обчислювальних машин, систем чи комп'ютерних мереж у зв'язку з виконуваною роботою або займаною посадою, або шляхом несанкціонованого доступу, -

караються обмеженням волі на строк до п'яти років або позбавленням волі на строк від трьох до п'яти років.

3. Дії, передбачені частинами першою чи другою цієї статті, якщо вони спричинили тяжкі наслідки, -

караються позбавленням волі на строк від п'яти до восьми років.

Примітка. У статтях 361 та 362 повторним визнається злочин, вчинений особою, що раніше вчинила будь-який із злочинів, передбачених цими статтями цього Кодексу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Азаров Д. Порушення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації //Право України. – 2000. – № 12. – С. 69 – 73.
2. Аналітичний огляд стану комп'ютерної злочинності та інформаційної безпеки в Україні у 2000 році // Національне бюро Інтерполу в Україні. – К., 2001. – 26 с.
3. Антонов С. Компьютерные преступления в банковской сфере // Юридическая практика. – 1997. - №8. - С. 7.
4. Бажанов М.И. Множественность преступлений по уголовному праву Украины. – Х.: Право, 2000. – 128 с.
5. Бажанов М.И. Уголовное право Украины. Общая часть. – Днепропетровск: Пороги, 1992. – 168 с.
6. Баранов О.А. Проблеми законодавчого забезпечення боротьби з комп'ютерними злочинами //Інформаційні технології та захист інформації: Збірник наукових праць. – Запоріжжя: Юридичний інститут МВС України, 1998. – Вип. 2.
7. Батурин Ю.М. Компьютерное право: краткий реестр проблем //Советское государство и право. – 1988. – № 8.
8. Батурин Ю.М. Проблемы компьютерного права. – М.: Юридическая литература, 1991. – 271 с.
9. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юридическая литература, 1991. - 160 с.
10. Батурин Ю.Н., Жодзишский А.М. Компьютерные правонарушения: криминализация, квалификация, раскрытие //Советское государство и право. – 1990. – № 12. – С. 86 – 95.
11. Бачинин В.А. Философия права и преступления. – Харьков: Фолио,

1999. – 560 с.

12. Бекария Чезаре. О преступлениях и наказаниях. – М: Юр. Издат., 1939. – 463 с.
13. Белогриц-Котляревский Н.С. Учебник русского уголовного права. Общая и Особенная части. Украинское книгоиздательство – Киев – Петербург. – Харьков, 1903. – 618 с.
14. Бидашко Е.А., Волкова Н.Л. Компьютерные преступления: миф или реальность? // Нуковий вісник Дніпропетровського юридичного інституту МВС України. – 2001. – № 1 (14). – С. 160 –168.
15. Біленчук П.Д., Зубань М.А., Комп'ютерні злочини: соціально-правові та кримінолого-криміналістичні аспекти: Навчальний посібник. – К.: Українська академія внутрішніх справ, 1994. – 72 с.
16. Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп'ютерна злочинність: Навчальний посібник. – К.: Атіка, 2002. – 204 с.
17. Вакка Дж. Секреты безопасности в Internet. – К.: Диалектика, 1997. – 512 с.
18. Венгеров А.Б. Категория "информация" в понятийном аппарате юридической науки //Советское государство и право. – 1977. – № 10.
19. Венгеров А.Б. Право и информатика в условиях автоматизации управления (Теоретические вопросы). – М. Юридическая литература, 1978.
20. Вертузаев, А. Попов Предупреждение компьютерных преступлений и их расследование //Право Украины. – 1998. – № 1. – С. 101 – 103.
21. Вехов В.В. Компьютерные преступления: Способы совершения и раскрытия /Под ред. акад. Б.П. Смагоринского. – М.: Право и Закон, 1996. – 182 с.
22. Винер Н. Кибернетика или управление и связь в животном и машине. – М.: Советское радио, 1968. – 328 с.

23. Винер Н. Кибернетика. – М., 1983. – 352 с.
24. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО Изд-во “Юрлитинформ”, 2002. – 496 с.
25. Волков Б.С. Мотивы преступлений (Уголовно-правовое и социально-пси-хологическое исследование). – М.: Издательство казанского универ-ситета, 1982. – 152 с.
26. Волков Б.С. Проблема воли и уголовная ответственность. – Казань: Изд-во КГУ, 1963. – 135 с.
27. Волобуєв А.Ф. Особливості розслідування розкрадань грошових коштів, що здійснюються з використанням комп’ютерної техніки //Вісник Луганського інституту внутрішніх справ. – 1998. – № 2. – С. 179 – 185.
28. Воройский Ф.С. Систематизированный толковый словарь по информатике (Вводный курс по информатике и вычислительной технике в терминах). – М.: Киберия, 1998. – 520 с.
29. Воры проникли в компьютерную сеть Национального банка //Голос Украины. – 1998. – 5 ноября. – № 217 (1963). – С. 2.
30. Гавловський В.Д., Цимбалюк В.С. Щодо проблем боротьби із злочинами, що вчинюються з використанням комп’ютерних технологій //Уряду України. Президенту, законодавчій, виконавчій владі "Боротьба з контрабандою: проблеми та шляхи їх вирішення". Аналітичні розробки, пропозиції наукових і практичних працівників /Керівники авторського колективу А.І. Комарова, О.О. Крикун. – К., 1998. – С. 148 – 154.
31. Гавриленко І. Комп’ютерна злочинність // Юридичний вісник України. – 1997. – № 28.
32. Гаврилов О.А. Информатизация правовой системы России.

Теоретические и практические проблемы. – М., 1998. – 223 с.

33. Гаврилов О.А. Компьютерные технологии в правотворческой деятельности: Учебное пособие. – М.: ИНФРА М, 1999. – 108 с.

34. Гаврилов О.А. Курс правовой информатики: Учебник для вузов. – М.: Издательство НОРМА, 2000. – 419 с.

35. Глистер Пол. Новый Навигатор Internet. – К.: Диалектика, 1996. – 554 с.

36. Голина В.В., Пивоваров В.В. Проблемы компьютерной преступности //Фінансова злочинність: Зб. Матеріалів міжнар. наук.-практ. семінару [Харків], 12-13 лют. 1999 р. /[Редкол.: Борисов В.І. (голов. ред.) та ін.]. – Х.: Право, 2000. - С. 62 –73.

37. Голубев В.В., Дубров П.А., Павлов Г.А. Компьютерные преступления и защита информации в вычислительных системах //Защита информации. – М.: Знание, 1990.

38. Голубєв В.О. Правові проблеми захисту інформаційних технологій // Вісник Запорізького юридичного інституту. –1997. – № 2. – С. 35 – 40.

39. Голубєв В.О. Теоретично-правові проблеми боротьби з комп’ютерною злочинністю // Вісник Запорізького юридичного інституту. –1999. – № 3. – С. 52 – 60.

40. Гриднева М. Змей из Интернета //Московский комсомолец. – 1999. – 14 ноября. – С. 6 – 7.

41. Гуцалюк М. Координація боротьби з комп’ютерною злочинністю // Право України. – 2002. – № 5. – С. 121 – 126.

42. Дагель П.С., Котов Д.П. Субъективная сторона преступления и ее установление. – Воронеж, 1974. – 244 с.

43. Дагель П.С., Михеев Р.И. Теоретические основы установления вины: Учебное пособие. – Владивосток, 1975. –168 с.

44. ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. Від

01.07.94.

45. ДСТУ 2938-94 Системи оброблення інформації. Основні положення. Терміни та визначення. Від 01.01.96.

46. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. Від 01.01.1998.

47. Дубовая Л. Остерегайтесь компьютерных злоумышленников //Computer World. – Киев, 1995. – № 41(62). – 18 октября.

48. Дурманов Н.Д. Понятие преступления. – М.- Л.: Издательство АН СССР, 1948. – 311 с.

49. Дьяконов С.В., Игнатьев А.А., Лунеев В.В., Никулин С.И. Уголовное право. – М.: Издательская группа Норма-Инфра М, 1999. – 416 с.

50. Закон України "Про державну таємницю" від 21.01.1994 року //Закони України. Т. 7. – К., 1997. – С. 38 – 50.

51. Закон України "Про захист інформації в автоматизованих системах" // Відомості Верховної Ради України. –1994. – № 31. – Ст. 286.

52. Закон України "Про інформацію" від 2.11.1992 року //Закони України. Т. 4. – К., 1996. – С. 72 – 87.

53. Закон України "Про підприємства в Україні" від 22.03.1991 року //Закони України. Т. 1. – К., 1995. – С. 191 – 199.

54. Иванов В.Г., Коровин А.С. Алгоритм защиты и сжатия файлов // Правові основи захисту комп’ютерної інформації від протиправних посягань. Матеріали міжвузівської науково-практичної конференції (22 грудня 2000 року). - Донецьк: Донецький інститут внутрішніх справ, 2001. – С. 212 –215.

55. Кабанников А. Личный хакер Клинтона отправляется в тюрьму //Комсомольская правда. – 1999. – 24 ноября. – С. 3.

56. Кабанников А. Электронная “Хиросима” уже затаилась в Москве // Комсомольская правда. – 1998. – 16 декабря. – С. 5.

57. Калюжный Р.А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект): Автореф. дисс. … д-ра юрид. наук: 12.00.02 /АН Украины, Институт государства и права им. В.М. Корецкого. – К., 1992. – 47 с.

58. Клаус Г. Кибернетика и общество. – М., 1967. – 242 с.

59. Коваленко М.М. Комп’ютерні віруси і захист інформації. – К.: Наукова думка, 1999. – 268 с.

60. Комментарий к Уголовному кодексу Российской Федерации – М.: Проспект, 1997. – 760 с.

61. Комментарий к Уголовному кодексу Российской Федерации /Отв. ред. д-р юрид. наук, проф. А.В. Наумов. – М.: Юристъ, 1996. – 824 с.

62. Комментарий к Уголовному кодексу Российской Федерации /Отв. ред. В.И. Радченко. – М.: Вердикт, 1996. – 412 с.

63. Комментарий к Уголовному кодексу Российской Федерации. Издание 2-е, измененное и дополненное /Под общ. ред. Ю.И. Скуратова и В.М. Лебедева. – М.: Издательская группа Норма - Инфра М, 1998. – 832 с.

64. Компьютерные террористы: новейшие технологии на службе преступного мира /Авт.-сост. Т.И. Ревяко. – Минск: Литература, 1997. – 640 с.

65. Компьютерные технологии в юридической деятельности. Учебное и практическое пособие / Под ред. Н.Полевого, В. Крылова. - М., 1994. - 250 с.

66. Корж Ю. Інтернет в Україні //Вісник НАН України. – 1999. – № 1. – С. 54 – 58.

67. Кретов Б.И. Средства массовой коммуникации – элемент политической системы общества //Социально-гуманитарные знания. –

2000. – № 1. – С. 101 – 118.

68. Кривоченко Л.Н. Классификация преступлений. –Х.: Издательство при Харьковском государственном университете издательского объединения "Вища школа", 1983. – 129 с.

69. Кригер Г.А. Советское уголовное право. Общая часть: Учебник. – М: Изд-во МГУ, 1988. – 472 с.

70. Кримінальне право України. Загал. Частина: Підручник для студентів вузів і факультетів /Г.В. Андрусів, П.П. Андрушко, В.В. Бенківський та ін.; За ред. П.С. Матишевського та ін. – К.: Юрінком Інтер, 1997. – 512 с.

71. Кримінальне право України: Загальна частина: Підручник для студентів юрид. спец. вищ. закладів освіти /М.І. Бажанов, Ю.В. Баулін, В.І. Борисов та ін.; За ред. професорів М.І. Бажанова, В.В. Сташиса, В.Я. Тація. – Київ-Харків: Юрінком Інтер-Право, 2001. – 416 с.

72. Кримінальне право України: Особлива частина: Підручник для студентів юрид. спец. вищ. закладів освіти /М.І. Бажанов, В.Я. Тацій, В.В. Сташис, І.О. Зінченко та ін.; За ред. професорів М.І. Бажанова, В.В. Сташиса, В.Я. Тація. – Київ-Харків: Юрінком Інтер-Право, 2001. – 496 с.

73. Кримінальне право України: Особлива частина: Підручник для студентів юридичних вузів і факультетів /Г.В. Андрусів, П.П. Андрушко, С.Я. Лихова та ін.; За ред. П.С. Матишевського та ін. – К.: Юрінком Інтер, 1999. – 896 с.

74. Кримінальний кодекс України // Відомості Верховної Ради України. – 2001. - № 25 – 26. – Ст. 131.

75. Кругликов Л.Л., Савинов В.Н. Квалифицирующие обстоятельства: понятие, виды, влияние на квалификацию преступлений: Учебное пособие. – Ярославль: Ярославский университет, 1989. – 86 с.

76. Крылов В.В. Информационные компьютерные преступления. – М.: Издательская группа Инфра М - Норма, 1997. – 285 с.
77. Кудрявцев В.Н. Объективная сторона преступления. – М.: Госюриздат, 1960. – 245 с.
78. Кузнецов А. Пираты в Интернете //Милиция. – 2000. – № 2. – С. 26 – 27.
79. Кузнецов Н.А., Мусхелишвили Н.Л., Шрейдер Ю.А. Информационное взаимодействие как объект научного исследования //Вопросы философии – 1999. – № 2. – С. 77 – 87.
80. Кузнецова Н.Ф. Значение преступных последствий для уголовной ответственности. – М.: Государственное издательство юридической литературы, 1958. – 219 с.
81. Кузнєцов В. Комп'ютерна інформація як предмет крадіжки //Право України. – 1999. – № 7. – С. 85 – 88.
82. Кураков Л.П., Смирнов С.Н. Информация как объект правовой защиты. – Гелиос, 1998. –240 с.
83. Курс уголовного права. Общая часть. Том 1: Учение о преступлении: Учебник для вузов /Под ред. Н.Ф. Кузнецовой, И.М. Тяжковой. – М.: Зерцало, 1999. – 592 с.
84. Лісовий В. "Комп'ютерні" злочини: питання кваліфікації //Право України. – 2002. – № 2. – С. 86 – 88.
85. Логвиненко Н.Ф.,Емельянов С.Л., Носов В.В., Писаревский В.И. Современные методы и средства защиты компьютерной информации от утечки по электрическим каналам // Правові основи захисту комп'ютерної інформації від протиправних посягань. Матеріали міжвузівської науково-практичної конференції (22 грудня 2000 року). - Донецьк: Донецький інститут внутрішніх справ, 2001. – С. 190 –199.
86. Лысов Н.Н. Содержание и значение криминалистической

характеристики компьютерных преступлений // Проблемы криминалистики и методики ее преподавания (тезисы выступлений участников семинара-совещания преподавателей криминалистики). – М., 1994. – С. 54.

87. Ляпунов Ю., Максимов В., Ответственность за компьютерные преступ-ления //Законность. – 1997. – № 1. – С. 8 – 15.

88. Милкус А. Скромный компьютерщик опаснее атомной бомбы // Комсомольская правда. – 2000. – 11 мая. – С. 3.

89. Михлин А.С. Последствия преступления – М.: Юридическая литература, 1969. – 104 с.

90. Науково-практичний коментар до Кримінального кодексу України: за станом законодавства і постанов Верховного Суду України на 1 грудня 2001 р. / За ред. С. С. Яценка – К.: А. С. К., 2002. – 936 с.

91. Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001 року /За ред. М.І. Мельника, М.І. Хавронюка. – К.: Канон, 2001. – 1104 с.

92. Науково-практичний коментар Кримінального кодексу України: за станом постанов Пленуму Верховного Суду України на 1 січня 1997 р. /За ред. В.Ф. Бойка, Ю.М. Кондратьєва, С.С. Яценка. – К.: Юрінком, 1997. – 960 с.

93. Наумов А.В. Применение уголовно-правовых норм. – Волгоград, 1973. – 150 с.

94. Наумов А.В. Уголовное право. Общая часть: Курс лекций. – М.: БЕК, 1996. – 560 с.

95. Новиков О.А., Мясникова Л.А. Логистика и коммерция информационного общества //Проблемы развития внешнеэкономических связей и привлечения иностранных инвестиций: региональный аспект: Сборник научных трудов. – Донецк, 1999. – С.

117 – 121.

96. Новосёлов Г.П. Учение об объекте преступления. Методологические аспекты. – М.: Норма, 2001. – 203 с.

97. Новый уголовный кодекс Франции /Науч. ред. Н.Ф. Кузнецова, Э.Ф. Побегайло. – М., 1994.

98. Овчинский В.С. XXI век против мафии. Криминальная глобализация и Конвенция ООН против транснациональной организованной преступнсти. – М.: ИНФРА-М, 2001. – 148 с.

99. Панов Н.И. Оценочные понятия и их применение в уголовном праве //Проблемы социалистической законности: Республ. межвед. научн. сб. Вып. 7. – Х.: Вища школа, 1981. – С. 99 – 106.

100. Панов Н.И. Способ совершения преступления и уголовная ответственность. – Х.: Вища школа, 1982. – 160 с.

101. Першиков В.И., Савинков В.М. Толковый словарь по информатике. – М.: Финансы и статистика, 1991. – 543 с.

102. Пинаев А.А. Уголовно-правовая борьба с хищениями. – Х.: Издательское объединение "Вища школа", 1975. – 189 с.

103. Пионтковский А.А. Учение о преступлении. – М.: Госюриздат, 1961. – 655 с.

104. Питецкий В. Конкретизация оценочных признаков уголовного законодательства //Советская юстиция. – 1991. – № 2. – С. 6 – 7.

105. Питецкий В. Оценочные понятия в уголовном законе //Советская юстиция. – 1988. – № 12. – С. 7.

106. Полевой Н.С. и др. Правовая информатика и кибернетика: Учебник. – М.: Юридическая литература, 1993. – 496 с.

107. Положение по обеспечению безопасности компьютерных информационных систем в КНР //Борьба с преступностью за рубежом (по материалам зарубежной печати) //Ежемесячный информационный

бюллетень – М.: 1996. – № 9.

108. Постанова пленуму Верховного Суду "Про практику розгляду судами кримінальних справ про виготовлення або збут підроблених грошей або цінних паперів" від 12 квітня 1996 року № 6 // Збірник постанов Пленуму верховного Суду України кримінальних справах. – Х.: “Одісей”, 2000.- С. 155 - 159.

109. Постанова пленуму Верховного Суду "Про судову практику у справах про корисливі злочини проти приватної власності" № 12 від 25 грудня 1992 року // Збірник постанов Пленуму верховного Суду України кримінальних справах. – Х.: “Одісей”, 2000.- С. 131 - 147.

110. Постанова пленуму Верховного Суду "Про судову практику у справах про хабарництво" від 7 жовтня 1994 року № 12 // Збірник постанов Пленуму верховного Суду України кримінальних справах. – Х.: “Одісей”, 2000.- С. 219 - 230.

111. Постанова пленуму Верховного Суду України "Про судову практику у справах про злочини проти життя" № 1 від 1 квітня 1994 року // Збірник постанов Пленуму верховного Суду України кримінальних справах. – Х.: “Одісей”, 2000.- С. 96 – 113.

112. Постанова Пленуму Верховного Суду України № 4 від 2 липня 1976 року "Про питання, що виникли в судовій практиці у справах про знищення та пошкодження державного і колективного майна шляхом підпалу або внаслідок порушення правил пожежної безпеки" // Бюлетень законодавства і юридичної практики України. – 1995. – № 1. – 472 с.

113. Ракитов А.И. Философия компьютерной революции. – М.: Политиздат, 1991. - С. 260 с.

114. Расследование неправомерного доступа к компьютерной информации / Под. ред. Н.Г. Шуруханова. – М.: Щит – М, 1999. – С. 38

– 254 с.

115. Розенфельд Н. Відповідальність за незаконне втручання в роботу ЕОМ (комп'ютерів) // Вісник прокуратури. - 2002. - №4. - С. 23 – 27.

116. Российское уголовное право. Особенная часть / Под ред. В.Н. Кудрявцева, А.В. Наумова. – М.: Юристъ, 1997. – 524 с.

117. Российское уголовное право. Особенная часть: Учебник /Под ред. М.П. Журавлева, С.И. Никулина. – М.: Спарк, 1998. – 495 с.

118. Салтевський М.В. Основи методики розслідування злочинів, скоєних з використанням ЕОМ. Навчальний посібник. – Харків: Нац. юрид. акад. України, 2000. – 35 с.

119. Свиридов С. "Капкан" для хакера // Комсомольская правда. – 2002. – 10 сентября. – С. 5.

120. Северин В.А. Правовое регулирование информационных отношений //Вестник МГУ. Серия 11. Право. – 2000. – № 5.

121. Семилетов С.И. Информация как особый нематериальный объект права //Государство и право. – 2000. – № 5. – С. 67 – 74.

122. Семухин И.Ю. Информация – фактор общественного воспроизводства // Матеріали II звітної науково-практичної конференції професорсько-викладацького та курсантського складу Кримського факультету Університету внутрішніх справ. – Сімферополь: Доля, - 2000.

123. Сергеев В.В. Компьютерные преступления в банковской сфере // Банковское дело. - 1997. - № 2. - С 27. – 28.

124. Сирота С.И. Преступления против социалистической собственности и борьба с ними. – Воронеж: Издательство Воронежского университета, 1968. – 148 с.

125. Скоромников К.С. Компьютерное право Российской Федерации. – М.: Издательство МНЭПУ, 2000. – 224 с.

126. Словарь по кибернетике /Под ред. акад. В.М. Глушкова. – К.: Главная редакция Украинской Советской энциклопедии, 1979. – 420 с.

127. Снегірьов О.П., Голубєв В.О. Проблеми класифікації злочинів у сфері комп'ютерної інформації //Вісник університету внутрішніх справ. Вип. 5. – Х., 1999. – С. 25 – 28.

128. Суханов Е.А. Курс лекций по гражданскому праву. – М.: 1987. – 253 с.

129. Таганцев Н.С. Русское уголовное право: Лекции. Часть общая. В 2-х томах. Т. 1. – М., 1994. – 380 с.

130. Тарарухин С.А. Квалификация преступлений в следственной и судебной практике. – К.: Юринком, 1995. – 208 с.

131. Тарасенко Ф.П. К определению понятия "информация" в кибернетике //Вопросы философии. – 1963. – № 4. – С. 76 – 84.

132. Таций В.Я. Объект и предмет преступления в советском уголовном праве. – Х.: Вища шк.: Изд-во при ХГУ, 1988. – 198 с.

133. Терещенко Л.К. Информация и собственность //Защита прав создателей и пользователей программ для ЭВМ и баз данных (комментарий российского законодательства). – М., 1996.

134. Трайнин А.Н. Состав преступления по советскому уголовному праву. – М.: Государственное издательство юридической литературы, 1951. – 388 с.

135. Уголовное право России. Особенная часть: Учебник /Отв. ред. д-р юрид. наук, проф. Б.В. Здравомыслов. – М.: Юристъ, 1999. – 522 с.

136. Уголовное право России. Особенная часть: Учебник /Под ред. проф. А.И. Рарога. – М.: Институт международного права и экономики им. А.С. Грибоедова, 1998. – 480 с.

137. Уголовное право России. Учебник для вузов в 2-х томах. Т. 2. Особенная часть /Под ред. А.Н. Игнатьева, Ю.А. Красикова. – М.: Изд.

группа Норма – Инфра М, 1998. – 808 с.

138. Уголовное право. Общая часть: Учебник для вузов /Отв. ред. д-р юрид. наук, проф. И.Я. Козаченко и д-р юрид. наук, проф. З.А. Незнамова. – М.: Издательская группа ИНФРА М – НОРМА, 1997. – 516 с.

139. Уголовное право. Особенная часть: Учебник /Под ред. проф. А.И. Рарога. – М.: Институт международного права и экономики. Издательство "Триада, Лтд", 1997.

140. Уголовный кодекс Республики Беларусь / Вступ. Ст. А.И. Лукашова, Э.А. Саркисовой. – 2-е изд., испр. и доп. – Мн.: Тесей, 2001. – 312 с.

141. Уголовный кодекс Украины. Комментарий /Под ред. Ю.А. Кармазина и Е.Л. Стрельцова. – Х.: ООО "Одиссей", 2001. – 960 с.

142. Уголовный кодекс Украины: Научно-практический комментарий /Отв. Ред. С.С. Яценко, В.И. Шакун). – К.: Правові джерела, 1998. – 1088 с.

143. Уголовный кодекс ФРГ /Пер. с нем. А.В. Серебренникова. – М., 1996. – 156 с.

144. Указ Президента України № 928 від 31 липня 2000 року "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет і забезпеченню широкого доступу до цієї мережі в Україні" // Офіційний Вісник України. - № 31. - 2000. - Ст. 1300.

145. Украинцев Б.С. Информация и отражение //Вопросы философии. – 1963. – № 2. – С. 26 – 38.

146. Утевский Б.С. Общее учение о должностных преступлениях. – М.: Юридическое издательство, 1948. – 140 с.

147. Фесенко Є.В. Цінності як об’єкт злочину//Право України. – 1999. – № 6. – С. 75 – 78.

148. Философия: Учебник для высших учебных заведений. – Ростов-на-

Дону: Феникс, 1995. – 486 с.

149. Філософський словник / За ред. В.І. Шинкарука. – К.: Головна редакція УРЕ. 1973. – 600 с.

150. Флетчер Дж., Наумов А.В. Основные концепции современного уголовного права. – М: Юристъ, 1998. – 512 с.

151. Фролов В.С., “Думающее” оружие. - М.: Знание, 1991. (Новое в жизни, науке и технике. Сер. “Радиоэлектроника и связь”; № 7). – 62 с.

152. Фролов Е.А. Спорные вопросы общего учения об объекте преступления: Сборник ученых трудов. – Вып. 10. – Свердловск, 1969.

153. Церетели Т.В. Причинная связь в уголовном праве. – М.: Государственное издательство юридической литературы, 1963. – 382 с.

154. Черных А.В. Обеспечение безопасности автоматизированных информационных систем (уголовно-правовые аспекты) //Советское государство и право. – 1990. – № 6. – С. 116 – 121.

155. Черных А.В. Преступления компьютерного века // Советская юстиция. - 1987. - №11. - С 30 - 32.

156. Чечко Л. “Компьютерные” хищения //Российская юстиция. – 1996. – № 5. – С. 45.

157. Шевченко Є.В. Злочини з похідними наслідками в кримінальному праві: Автореф. дис. … канд. юрид. наук: 12.00.08 /Національна юридич-на академія України ім. Я. Мудрого. – Х., 2002. – 18 с.

158. Шершеневич Т.Ф. Учебник русского гражданского права (по изданию 1907 г.). – М.: Фирма "Спартак", 1995. – 556 с.

159. Шилан Н.Н., Кривонос Ю.М., Бирюков Г.М. Компьютерные преступления и проблемы защиты информации: Монография. – Луганськ: РИО ЛИВД, 1999. – 60 с.

160. Draft Convention on Cyber-crime and Explanatory memorandum related thereto: final activiti report. – Prapareted by Committee of Experts on Crime

in Cyber-Space (PC-CY) Submitted to European Committee on Crime Problems (CDPC) at its 50th plenary session (18 – 22 June 2001). – Secretariat Memorandym preparated by the Directorate General of Legal Affairs. – Restricted, CDPC (2001) 2 rev. 2. – Strasbourg, 20 June 2001.

161. Former Computer Network Administrator Guilty of Unleashing $10 Million Programming "Timebomb" (May 9, 2000), http://www.usdoj.gov/ criminal /cybercrime/njtime.html.

162. International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime, paragraph 86-87,http://www.ifs.univie.ac.at/~pr2qq/rew4344.html.

163. Israeli Citizen Arrested in Israel for Hacking United States and Israeli Government Computers (March 18, 1998), http://usdoj.gov/criminal/ cybercrime/ehudpr.html

164. Juvenile Computer Hacker Cuts off FAA Tower at Regional Airport - First Federal Charges Brought Against a Juvenile for Computer Crime (March 18, 1998), http://www.usdoj.gov/crimrnal/cybercrime/ juvenilepld.html

165. Stein Schjolberg, Chief Judge Moss byrett, Norway "The Legal Framework – Unauthorized Access to Computer Systems. Penal Legislation in 37 Countries", http://www.mossbyrett.of.no/legal.html.

166. The National Information Infrastructure Protection Act of 1996 Legislative Analysis By The Computer Crime and Intellectual Property Section United States Department of Justice, http://www.usdoj.gov/ criminal/cybercrime /1030_anal.html