

НАЦІОНАЛЬНА ЮРИДИЧНА АКАДЕМІЯ УКРАЇНИ
імені ЯРОСЛАВА МУДРОГО

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

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата юридичних наук

Харків - 2003

Дисертацією є рукопис.

Робота виконана на кафедрі кримінального права та кримінології Луганської академії внутрішніх справ МВС ім. 10-річчя незалежності України.

Науковий керівник -

кандидат юридичних наук, професор

Кривоченко Людмила Миколаївна,

Національна юридична академія України імені Ярослава Мудрого, в.о. завідувача кафедри кримінального права

Офіційні опоненти:

доктор юридичних наук, професор

Голіна Володимир Васильович,

Національна юридична академія України імені Ярослава Мудрого, завідувач кафедри кримінології і кримінально-виконавчого права.

доктор юридичних наук, професор

Костенко Олександр Миколайович,

Інститут держави і права ім. В.М. Корецького Національної академії наук України, завідувач відділу проблем кримінального права, кримінології та судоустрою;

Провідна установа -

Національна академія внутрішніх справ України, кафедра кримінального права, м. Київ.

Захист відбудеться " 14 " березня 2003 року о 10 годині на засіданні спеціалізованої вченої ради Д 64.086.01 у Національній юридичній академії імені Ярослава Мудрого за адресою: 61024, м. Харків, вул. Пушкінська, 77.

З дисертацією можна ознайомитися в бібліотеці Національної юридичної академії України імені Ярослава Мудрого за адресою: 61024, м. Харків, вул. Пушкінська, 77.

Автореферат розісланий "12" лютого 2003 р.

Вчений секретар
спеціалізованої вченої ради

Шепітько В.Ю.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

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 ХХ 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. Вехов, О.Г. Волеводз, О.А. Гаврилов, В.В. Голина, 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. Полевой, В.А. Северин, С.І. Семилетов, 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 підготовванні 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).

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовується актуальність теми дисертації, визначаються її мета та завдання, характеризуються методи дослідження, методологічна основа, структура, науково-практичне значення.

Перший розділ "Об'єкт і предмет незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж" містить чотири підрозділи.

У **підрозділі 1.1 "Проблема об'єкта злочину в науці кримінального права"** дається короткий аналіз проблеми визначення об'єкта злочину в теорії кримінального права. У результаті дослідження різних поглядів учених на цю проблему автор доходить висновку, що найбільш обґрунтованим та універсальним залишається визначення об'єкта злочину як суспільних відносин, охоронюваних кримінальним законом. З урахуванням цього автором викладено основні теоретичні та методологічні передумови дослідження об'єкта незаконного втручання.

Підрозділ 1.2 "Родовий об'єкт незаконного втручання в роботу електронно-обчислювальних машин" присвячено дослідженню змісту суспільних відносин, охоронюваних нормами, які передбачені в розділі XVI КК "Злочини у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж".

На основі аналізу змін у суспільних відносинах на сучасному етапі, викликаних появою та розширенням сфери застосування комп'ютерної техніки, і висловлених у науці позицій з цього питання дисертантом пропонується таке визначення родового об'єкта незаконного втручання:

інформаційні відносини у сфері використання електронно-обчислювальних машин, систем або комп'ютерних мереж.

Досліджуючи категорію "інформаційні відносини", особливу увагу автор звертає на предмет цих відносин – інформацію. Її специфіка полягає в тому, що їй притаманні властивості як матеріальних, так і нематеріальних об'єктів, що відбивається у двох взаємопов'язаних категоріях - "інформація" і "носії 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 відображенням - категорією, котра означає особливий результат впливу однієї матеріальної системи на іншу: відтворення в іншій формі особливостей однієї системи в особливостях другої. Процеси отримання, перетворення, зберігання та передавання інформації відбуваються за допомогою матеріальних об'єктів (носіїв інформації), стан яких і виступає сигналом. Проте інформація не є властивістю самого сигналу, вона - властивість співвідношення, зв'язку між об'єктами, стан одного з яких є сигналом стану іншого. Виходячи з цього, дисертант робить висновок, що співвідношення понять "інформація" і "носії" можна визначити таким чином: *інформація є нематеріальним об'єктом, який включається в систему суспільних відносин через матеріальний об'єкт – носій інформації.*

Автор аргументує положення про те, що в інформаційних відносинах використовуються не природні властивості матеріального предмета - носія інформації, а його специфічні інформаційні властивості. Інформація, не будучи чимось самостійним, абсолютним, має інформаційний характер тільки відносно системи, яка сприймає інформацію. У цьому полягає основна відмінність інформації від інших предметів суспільних відносин. Важливим тут є те, що соціально значущим у сфері правового регулювання суспільних відносин з приводу інформації є не просто володіння суб'єктом носієм інформації, а й наявність у нього можливості "одержати" інформацію з носія.

Визначивши родовий об'єкт злочинів у сфері використання електронно-обчислювальних машин, систем і комп'ютерних мереж, автор обґрунтовує необхідність введення такого терміна, як "комп'ютерний злочин" стосовно до злочинів, передбачених у розділі XVI КК України. Проаналізувавши наявні в науці визначення комп'ютерних злочинів, дисертант пропонує таке їх визначення: *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.*

У підрозділі 1.3 "**Безпосередній об'єкт незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж**" автор обґрунтовує, що безпосереднім об'єктом аналізованого злочину є суспільні відносини власності на комп'ютерну інформацію як частина інформаційних відносин.

Безпосередній об'єкт аналізованого злочину визначається дисертантом 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.*

У підрозділі 1.4 "**Предмет незаконного втручання**" розглядається поняття предмета незаконного втручання, його види. Закон вирізняє три предмети аналізованого злочину: комп'ютерна інформація, носій комп'ютерної інформації, комп'ютерний вірус.

Ознаки, що характеризують комп'ютерну інформацію як предмет злочину, автор співвідносить 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 середовища, фізичні, хімічні чи інші властивості яких використовуються для зберігання або передавання інформації, яка розпізнається 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 характеризується тим, що вона є чужою для винного і має власника.

Виходячи з викладеного, комп'ютерну інформацію як предмет злочину автор визначає як *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*.

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

Досліджуючи зміст поняття "комп'ютерний вірус", автор доходить таких висновків: 1) незважаючи на безліч різних підходів до визначення комп'ютерного вірусу, досі чіткої його дефініції немає; 2) найбільш обґрунтованим слід вважати, що комп'ютерний вірус являє собою комп'ютерну програму, спеціально призначену для знищення або перекинування 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 перекинування або знищення інформації. Це дозволило автору зробити 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 перекинування або знищення інформації (шкідливі програмні й технічні засоби)*.

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

Технічні засоби, 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 перекинування, іншого порушення права власності на неї.

Другий розділ "Об'єктивна сторона незаконного втручання в роботу електронно-обчислювальних машин, систем, комп'ютерних мереж". Аналіз диспозиції статті 361 КК дає можливість позначити, насамперед, законодавчу характеристику об'єктивної сторони незаконного втручання, яка можлива у двох різних формах:

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

Істотна різниця між цими формами вимагає самостійного розгляду їх змісту, обов'язкових ознак.

Підрозділ 2.1 "Незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж, яке призвело до перекинування або знищення комп'ютерної інформації" присвячений аналізу першої з цих форм. Виходячи з законодавчої конструкції, зазначена форма незаконного втручання є злочином з матеріальним складом, тобто обов'язковими ознаками об'єктивної сторони в даному випадку є діяння, наслідок і причинний зв'язок.

Діяння в цій формі виражається у втручанні в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж, яке є незаконним. Автор визначає його 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.

У даному підрозділі автором розглядається також питання про спосіб вчинення незаконного втручання. Різноманітні способи незаконного втручання в роботу ЕОМ, систем, комп'ютерних мереж, виходячи з характеристики засобів, які застосовуються для вчинення незаконного втручання, класифікуються дисертантом: 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 автор вживає термін "несанкціонований доступ", визначаючи його таким чином: спосіб вчинення незаконного втручання в роботу ЕОМ, систем, комп'ютерних мереж, що полягає в отриманні можливості здійснювати різні дії з комп'ютерної інформацією, яка має специфічні технічні чи програмні засоби захисту від її знищення або перекручення. На підставі аналізу практики боротьби з комп'ютерними злочинами та зарубіжного кримінального законодавства автор робить висновок про підвищену суспільну небезпечність цього способу, яка зумовлюється тим, що: 1) для подолання заходів інформаційної безпеки технічного чи програмного характеру потрібні спеціальні знання, специфічні навички; 2) шкода власникові заподіюється не тільки у вигляді знищення або перекручення комп'ютерної інформації, але й в істотних матеріальних витратах, що зумовлюється необхідністю відновлення чи заміни системи захисту. Це й визначає доцільність виділення несанкціонованого доступу як кваліфікуючої ознаки складу незаконного втручання, передбаченого в ч. 2 ст. 361 КК України, зазначивши: "Ті самі дії ... вчинені шляхом несанкціонованого доступу до комп'ютерної інформації".

Диспозиція статті 361 КК України як обов'язкову ознаку об'єктивної сторони незаконного втручання в роботу електронно-обчислювальних машин, систем чи комп'ютерних мереж передбачає суспільно небезпечні наслідки - знищення або перекручення комп'ютерної інформації, поняття яких розкриваються дисертантом.

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, стає непридатною для задоволення інформаційної потреби особою, котра 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.

Розглядаючи причинний зв'язок як обов'язкову ознаку об'єктивної сторони аналізованої форми незаконного втручання в роботу електронно-обчислювальних машин, автор виходить із загальних положень теорії необхідного спричинення, відповідно до якої для наявності аналізованого складу обов'язковим є необхідний закономірний зв'язок між незаконним втручанням і знищенням або перекрученням інформації: незаконне втручання являє собою необхідну умову, без якої наслідки у вигляді знищення або перекручення інформації не настали б. Відсутність необхідного причинного зв'язку виключає об'єктивну сторону незаконного втручання.

Закінченим незаконне втручання буде з моменту настання суспільно небезпечних наслідків у вигляді знищення або перекручення інформації.

Підрозділ 2.2 "Розповсюдження шкідливих програмних і технічних засобів". Другу форму об'єктивної сторони незаконного втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж законодавець конструює як злочин із формальним складом. Ця форма незаконного втручання вважається закінченою 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 автором аналіз цієї форми об'єктивної сторони дозволив дійти висновку, що диспозиція статті 361 не охоплює повною мірою всі можливі способи вчинення цього злочину, які відомі в інформатиці та зустрічаються в практиці. У зв'язку з цим у дисертації пропонується нова редакція диспозиції ст. 361 КК у частині, що характеризує другу форму об'єктивної сторони незаконного втручання:

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

Таке формулювання дозволило б: 1) більш точно визначити предмет даного злочину, позначивши його як будь-які шкідливі програмні та технічні засоби (у тому числі комп'ютерні віруси); 2) удосконалити характеристику об'єктивної сторони даного злочину з точки зору засобів і способів вчинення розповсюдження комп'ютерних вірусів; 3) забезпечити більш ефективний захист інформаційних відносин і правильну кваліфікацію вчинених дій.

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 за допомогою комп'ютерних мереж; по-друге, у розповсюдженні шкідливих технічних засобів, тобто у їх оплатному або безоплатному передаванні, а також установленні в ЕОМ, системи чи комп'ютерні мережі.

У третьому розділі **"Суб'єктивні ознаки незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж"** аналізуються ознаки суб'єктивної сторони та суб'єкта даного злочину.

У підрозділі 3.1 **"Суб'єктивна сторона незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж"** автор обґрунтовує висновок, що вина в цьому складі може виражатися тільки в умислі, який може бути як прямим, так і непрямым.

Аналізуючи усвідомлення особою фактичних ознак вчинюваного злочину, автор доходить висновку, що таке усвідомлення полягає в розумінні винним у загальних рисах закономірностей функціонування ЕОМ: не потрібно, щоб винний охоплював свідомістю всі деталі складного процесу функціонування ЕОМ.

Серйозну увагу дисертант приділяє питанню усвідомлення винним протиправності своїх дій. В аналізованому складі воно виступає як необхідна ознака: вчиняючи незаконне втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж, суб'єкт злочину усвідомлює відсутність у нього права на комп'ютерну інформацію, а отже, порушення ним встановленого власником інформації порядку використання електронно-обчислювальних машин, систем і комп'ютерних мереж, тобто усвідомлює незаконність свого діяння.

Передбачення як інтелектуальна ознака умислу в цьому злочині охоплює не тільки розуміння можливості або неминучості наслідків, але й розуміння, хоча б у загальних рисах, причинного зв'язку між незаконним втручанням і знищенням або пошкодженням інформації, тим самим особа передбачає, що можливість власника здійснювати свої права на інформацію буде виключено або значно погіршено. Вольовий момент умислу при вчиненні незаконного втручання полягає в бажанні або свідомому допущенні таких наслідків. Про його наявність і зміст можуть свідчити характер дій, спосіб вчинення незаконного втручання, мотиви й мета, якими керується особа. Виходячи з цього, автор доводить, що в даному злочині умисел може бути як прямим, так і непрямым.

Аналізуючи суб'єктивну сторону розповсюдження шкідливих програмних чи технічних засобів як другої форми досліджуваного злочину, дисертант виходить із специфіки конструкції її об'єктивної сторони як злочину з формальним складом. Тому для наявності інтелектуальних ознак вини достатньо усвідомлення особою суспільної небезпечності розповсюдження шкідливих програмних чи технічних засобів, незаконності таких дій, а також розуміння того, що розповсюджені засоби спеціально призначені для незаконного втручання, тобто є шкідливими. Виходячи з того, що незаконне втручання в цій формі є формальним складом злочину, для

наявності вольового моменту достатньо бажання особи вчинити саме діяння – розповсюдження шкідливого програмного або технічного забезпечення.

У підрозділі 3.2 "**Суб'єкт незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж**" робиться висновок про те, що позиція законодавця про визнання суб'єктом незаконного втручання особи, яка досягла 16-ти років, є правильною та ґрунтується на складності об'єктивної сторони незаконного втручання. Автор аргументує недоцільність пропозицій, які зустрічаються в літературі, про зниження віку кримінальної відповідальності за ці злочини до 14-ти років.

Аналізуючи ознаки суб'єкта незаконного втручання, автор на основі кримінологічної характеристики осіб, які вчиняють даний злочин, доходить висновку, що здебільшого, як свідчить практика, незаконне втручання вчиняється особою, яка має *правомірний доступ* до комп'ютерної інформації. Це значно підвищує ступінь суспільної небезпечності вчинюваного злочину. Між тим діючий закон цього не враховує: такі дії осіб, котрі мають правомірний доступ до комп'ютерної інформації, кваліфікуються як просте незаконне втручання за ч. 1 ст. 361 КК. Виходячи з цього, автор пропонує доповнити ч. 2 ст. 361 КК України кваліфікуючою ознакою: вчинення незаконного втручання особою, яка має санкціонований доступ до роботи на ЕОМ, у системі чи комп'ютерній мережі у зв'язку з виконуваною роботою або займаною посадою.

У четвертому розділі "**Кваліфікуючі ознаки незаконного втручання в роботу електронно-обчислювальних машин**" досліджуються ознаки, передбачені в ч. 2 ст. 361 КК: незаконне втручання, яке спричинило істотну шкоду, вчинення незаконного втручання повторно чи за попередньою змовою групою осіб.

У підрозділі 4.1 "**Незаконне втручання, яке спричинило істотну шкоду**" автором аналізується зміст поняття істотної шкоди, спричиненої незаконним втручанням, та 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 у заподіянні матеріальної шкоди (позитивної чи упущеної вигоди), або в *іншій* нематеріальній шкоді, що, як правило, являє собою більш тяжкі наслідки, ніж матеріальна шкода. Такі наслідки можуть виражатися у поставленні в небезпеку або заподіянні шкоди життю та здоров'ю громадян, погіршенні обороноздатності держави, підриві авторитету державних органів, підприємств, установ чи організацій, зупиненні або порушенні складних технологічних процесів, безпеки руху тощо. Між тим з аналізу норм Особливої частини КК випливає, що законодавець (у переважній більшості складів) пов'язує істотну шкоду саме з матеріальною шкодою. А тому це дозволяє автору зробити висновок, що більш обґрунтованою, відповідною до специфіки об'єкта й об'єктивної сторони цього складу була б така кваліфікуюча ознака, як "настання тяжких наслідків". Отже, удосконалюючи ст. 361 УК України, доцільно виключити з ч. 2 поняття "істотна шкода", а доповнити її частиною 3, сформулювавши її таким чином: "*дії, передбачені частинами першою чи другою цієї статті, якщо вони спричинили тяжкі наслідки*".

У підрозділі 4.2 "**Вчинення незаконного втручання повторно**" аналізується зміст ознак повторного вчинення досліджуваного злочину, а також робиться висновок, що більш доцільним було б визнання незаконного втручання повторним у разі його вчинення не тільки після тотожного злочину, а й після вчинення однорідного злочину, передбаченого ст. 362 КК України "Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем". 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".

У підрозділі 4.3 "**Незаконне втручання, вчинене за попередньою змовою групою осіб**" особлива увага приділяється питанню незаконного втручання, вчиненого за попередньою змовою групою осіб. Це зумовлено тим, що КК України 2001 року вперше визначив форми співучасті за критерієм ступеня спільності участі. У цьому підрозділі визначаються критерії відмежування незаконного втручання, вчиненого групою осіб, від незаконного втручання, вчиненого за попередньою змовою групою осіб, і робиться висновок, що незаконне втручання, вчинене групою осіб, кваліфікується за ч. 1 ст. 361 КК України. Також зазначається, що вчинення незаконного

втручання організованою групою або злочинною організацією слід кваліфікувати за ч. 2 ст. 361 КК України, оскільки цим формам співучасті властиві всі ознаки вчинення незаконного втручання за попередньою змовою групою осіб.

У п'ятому розділі **"Відмежування незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж від суміжних складів злочину"** дисертант аналізує ознаки, які дозволяють відмежувати незаконне втручання від двох суміжних груп злочинів: по-перше, інших злочинів, передбачених розділом XVI КК, по-друге, від злочинів, пов'язаних із використанням комп'ютерної техніки як знаряддя або засобу вчинення злочину.

Підрозділ 5.1. "Відмежування незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж від інших комп'ютерних злочинів". Визначаючи критерії розмежування незаконного втручання та злочину, передбаченого ст. 362 КК України, дисертант доводить, що об'єктивна сторона незаконного втручання полягає в діях, у результаті яких комп'ютерна інформація, що є предметом злочину, перестає існувати або стає повністю чи частково непридатною для задоволення інформаційної потреби. А при вчиненні викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем комп'ютерна інформація не знищується і не перекручується, нею заволодіває суб'єкт злочину. При цьому вона, як правило, залишається у власника комп'ютерної інформації. Відмежування досліджуваного складу від злочину, передбаченого ст. 363 КК "Порушення правил експлуатації автоматизованих електронно-обчислювальних систем", є більш складним, оскільки стосується практично всіх об'єктивних і суб'єктивних ознак даних складів.

Підрозділ 5.2 "Відмежування незаконного втручання від злочинів, пов'язаних із використанням комп'ютерної техніки як знаряддя або засобу вчинення злочину". Основні відмінності незаконного втручання від злочинів проти власності полягають в ознаках об'єкта та предмета посягання. Безпосереднім об'єктом умисного знищення або пошкодження майна (ст. 194 КК України) є право власності на річ. У свою чергу, безпосередній об'єкт незаконного втручання визначено як право власності на інформацію. Різниця між даними суспільними відносинами полягає в тому, що перші є формою реалізації соціального інтересу щодо володіння, користування та розпорядження майном, а другі - інформацією. Відмінність між інформацією та річчю полягає, насамперед, у їх фізичній властивості (підрозділ 1.4 розділу 1). Також у цьому підрозділі визначаються критерії відмежування незаконного втручання від злочинів, передбачених ст. ст. 114, 200, 231, 224, 357 КК України.

У **висновках** відповідно до мети та завдань дослідження наводяться визначення родового та безпосереднього об'єктів незаконного втручання, предмета цього злочину, показується специфіка його суб'єктивної сторони, визначаються критерії відмежування незаконного втручання від суміжних злочинів, формулюються заключні положення, та пропонується нова редакція статті 361 КК України "Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), 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 ОПУБЛІКОВАНИХ ПРАЦЬ:

1. Карчевский Н.В. Уголовно-правовые аспекты влияния на общественные отношения развития компьютерных технологий //Проблеми вдосконалення законодавства та практика його застосування з урахуванням прогнозу злочинності: Вісник ЛІВС МВС України. Спеціальний випуск. - Ч. 3. – Луганськ: РВВ ЛІВС, 1999. – С. 112-117.

2. Карчевский Н.В. Уголовно-правовая охрана компьютерной информации // Вісник ЛІВС МВС України. - 2000. - № 2. - С. 91-104.

3. Карчевский Н.В. Преступления против собственности на компьютерную информацию: определение, объект и предмет //Вісник ЛІВС МВС України. - 2001. - № 1. – С. 33 – 48.

4. Карчевський М.В. Удосконалення кримінального законодавства України про комп'ютерні злочини в контексті законодавства зарубіжних країн //Вісник Університету внутрішніх справ. - 2001. - № 13. - С. 157-166.

5. Карчевский Н.В. Уголовная ответственность за незаконное вмешательство в работу электронно-вычислительных машин по новому Уголовному кодексу Украины //Вісник ЛІВС МВС України. - 2001. - № 3. - С. 143-156.

6. Карчевский Н.В. Компьютерная информация как предмет уголовно-правовой охраны //Правові основи захисту комп'ютерної інформації від протиправних посягань: Матеріали міжвузівської науково-практичної конференції (22 грудня 2000 року). - Донецький інститут внутрішніх справ, 2001. – С. 54 – 67.

7. Карчевський М.В. Визначення поняття "комп'ютерний злочин" //Конституція - основа державно-правового будівництва і соціального розвитку України: Тези доп. та наук. повідомлень учасників наук. конф. молодих учених (м. Харків, 30 червня 2001 р.) / За ред М.І. Панова. - Харків: Нац. юрид. акад. України, 2001. – С. 177 – 178.

8. Карчевський М.В. Незаконне втручання в роботу ЕОМ: питання кваліфікації за новим Кримінальним кодексом України // Нове кримінальне і кримінально-процесуальне законодавство та завдання юридичної підготовки кадрів ОВС України: Вісник ЛАВС МВС імені 10-річчя незалежності України. Спеціальний випуск. - Ч. 1. – Луганськ: РВВ ЛАВС, 2002. – С. 137-139.

9. Карчевський М.В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж: Монографія. - Луганськ: РВВ ЛАВС, 2002. - 144 с.

А Н О Т А Ц І Я

Карчевський М.В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину). – Рукопис.

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.08 - кримінальне право та криминологія; кримінально-виконавче право. - Луганська академія внутрішніх справ МВС імені 10-річчя незалежності України. - Луганськ, 2002.

У дисертації досліджуються ознаки складу злочину, передбаченого ст. 361 "Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж", визначаються критерії його відмежування від суміжних складів та формулюються пропозиції щодо вдосконалення цієї норми.

Обґрунтовується необхідність доповнення ч. 2 ст. 361 КК такими кваліфікуючими ознаками: несанкціонований доступ до комп'ютерної інформації та вчинення незаконного втручання особою, що має доступ до електронно-обчислювальних машин, систем чи комп'ютерних мереж у зв'язку з

виконуваною роботою або займаною посадою. Пропонується доповнення статті 361 частиною 3, яка б передбачала відповідальність за незаконне втручання, що спричинило тяжкі наслідки, а також приміткою, яка б містила вказівку на те, що незаконне втручання є повторним у випадку, якщо особа, яка його вчинила, раніше вчинила будь-який із злочинів, передбачених статтями 361 та 362 КК України.

Ключові слова: злочини у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж, комп'ютерна інформація, знищення, переключення, несанкціонований доступ.

А Н Н О Т А Ц И Я

Карчевский Н.В. Уголовная ответственность за незаконное вмешательство в работу электронно-вычислительных машин (компьютеров), систем и компьютерных сетей (анализ состава преступления). – Рукопись.

Диссертация на соискание ученой степени кандидата юридических наук по специальности 12.00.08 - уголовное право и криминология; уголовно-исполнительное право. - Луганская академия внутренних дел МВД имени 10-летия независимости Украины. - Луганск, 2002.

В диссертации исследуются признаки состава преступления, предусмотренного ст. 361 "Незаконное вмешательство в работу электронно-вычислительных машин, систем и компьютерных сетей", для его правильной квалификации и формулирования предложений по совершенствованию данной нормы.

В работе дается определение родового объекта преступлений в сфере использования электронно-вычислительных машин, систем и компьютерных сетей. Обосновывается вывод о том, что незаконное вмешательство является преступлением против собственности на компьютерную информацию. Предлагаются определения и признаки предметов незаконного вмешательства - компьютерной информации и вредоносных программных и технических средств. Аргументируется тезис о нецелесообразности признания предметом исследуемого преступления носителей компьютерной информации и компьютерных вирусов.

Диссертант выходит с предложением о необходимости изменения диспозиции ст. 361 УК в той части, где она описывает вторую форму незаконного вмешательства и предлагает следующую формулировку: "распространение программных и технических средств, предназначенных для незаконного проникновения в ЭВМ, системы или компьютерные сети и способных причинить искажение или уничтожение компьютерной информации"

Обосновывается необходимость дополнения ч. 2 ст. 361 УК такими квалифицирующими признаками: несанкционированный доступ к компьютерной информации и совершение незаконного вмешательства лицом, имеющим правомерный доступ к работе на ЭВМ в системе или компьютерной сети в связи с занимаемой должностью или специальными полномочиями. Предлагается дополнение статьи 361 частью 3, которая бы предусматривала ответственность за незаконное вмешательство, причинившее тяжкие последствия, а также примечанием, которое бы содержало указание на то, что незаконное вмешательство является повторным в случае, если лицо, его совершившее, ранее совершило любое из преступлений, предусмотренных статьями 361 и 362 УК Украины.

Ключевые слова: преступления в сфере использования электронно-вычислительных машин, систем и компьютерных сетей, компьютерная информация, уничтожение, искажение, несанкционированный доступ.

S U M M A R Y

Karchevsky M.V. Criminal responsibility for illegal interference into the computers` engineering work and the computer nets. - Manuscript

The thesis for a Candidate`s Degree in Law Sciences in specialty 12.00.08 - criminal law and criminology; criminal executive law. - Yaroslav Mudry National Law Academy of Ukraine. - Kharkiv, 2002.

The thesis is devoted to research of signs of corpus delicti provided for by Article 361 (Criminal Code of Ukraine) "Illegal interference into the computers` engineering work and the computer nets". The author specifies criterions wich draw a boundary line between corpus delicti and related one. He also formulates some propositions which are concerned with the improvement of given norm.

The necessity of addition part 2 article 361 (Criminal Code of Ukraine) is based by such skilled indication: unauthorized access into the computer`s information and committing illegal interference by person who has legal access into the computers` engineering work in the system or computer nets according to the office or special powers. The addition to the article 361, part 3 was offered, which would provide the responsibility for illegal interference having heavy consequences and also notes which contained the points to the fact, that illegal interference was repeated in case if the accused has committed any crime before which was provided for by articles 361 and 362 (Criminal Code of Ukraine).

Key words: computer crime, computer information, destruction, unauthorized access.

Відповідальний за випуск канд. юрид. наук, доц. Ю.О. Кучер

Підписано до друку 02.01.2003. Формат 60x90/16
Папір офсетний. Друк офсетний. Гарнітура Times.
Ум. друк. арк. 1,0. Обл.вид. арк. 1,0.
Тираж 100 прим. Зам. № 1

Редакційно-видавничий відділ ЛАВС МВС України
Імені 10-річчя незалежності України
Друкарня РВВ ЛАВС
91493, м. Луганськ, сел. Ювілейне, вул. К. Маркса, 4