МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

М. В. Карчевський

Злочини у сфері використання комп'ютерної техніки

Навчальний посібник

Рекомендовано
Міністерством освіти і науки України

Київ • Атіка • 2010

УДК 343.346.8:004](075)
ББК 67.408я7+32.973я7
К27

Рекомендовано
Міністерством освіти і науки України
як навчальний посібник для студентів вищих навчальних закладів
(Лист № 1.4/18-Г-3030 від 31.XII 2008 р.)

Рецензенти:

Костенко О. М.– доктор юридичних наук, професор, академік Академії правових наук України, завідувач відділу проблем кримінального права, кримінології та судоустрою Інституту держави і права імені В. М. Корецького НАН України, заслужений діяч науки і техніки України;

Розовський Б. Г.– доктор юридичних наук, професор, професор кафедри правознавства юридичного факультету Східноукраїнського національного університету імені Володимира Даля, заслужений юрист України.

Карчевський М. В.

К27 Злочини у сфері використання комп'ютерної техніки: Навчальний посібник.– К.: Атіка, 2010.– 168 с.

ISBN 978-966-326-353-3

У посібнику досліджуються ознаки складів злочинів, передбачених розділом XVI КК України (зі змінами, внесеними згідно із законами України від 05.06.2003 р. № 908-IV, від 23.12.2004 р. № 2289-IV), висвітлюються питання відмежування комп'ютерних злочинів від суміжних, пропонуються для обговорення можливі зміни до чинного кримінального законодавства.

Для студентів і курсантів юридичних вищих навчальних закладів та факультетів, а також слухачів магістратури.

УДК 343.346.8:004](075)
ББК 67.408я7+32.973я7

ISBN 978-966-326-353-3

ЗМІСТ

ПЕРЕДМОВА

«Кіберзлочинність», «хакери», «комп'ютерний злом», «крадіжка машинного часу» – ці терміни вже перестали бути екзотикою для юристів. Проблеми протидії злочинам у сфері використання комп'ютерної техніки активно обговорюються науковцями, досить швидко розвивається практика застосування відповідних норм законодавства про кримінальну відповідальність.

На сьогодні комп'ютерні злочини – це одна з найдинамічніших груп суспільно небезпечних посягань. Швидко збільшуються показники поширення цих злочинів, а також постійно зростає їх суспільна небезпечність. Це зумовлене прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки. Слід зауважити, що український законодавець приділяє значну увагу цій проблемі: 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»; двічі положення цього розділу змінювалися та доповнювалися (закони України «Про внесення змін до Кримінального кодексу України щодо відповідальності за незаконне втручання в роботу мереж електрозв'язку» від 5 червня 2003 р. та «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» від 23 грудня 2004 р.). Зростання суспільної небезпечності комп'ютерних злочинів та постійне оновлення кримінального законодавства з питань протидії їм краще за все свідчать про актуальність і своєчасність питань, що розглядаються в межах курсу «Злочини у сфері використання комп'ютерної техніки», який читається слухачам магістратури Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.

Метою курсу є ознайомлення слухачів магістратури з основними тенденціями та закономірностями розвитку кримінального законодавства про злочини у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж і мереж електрозв'язку; проблемами кваліфікації цих злочинів; напрямами вдосконалення кримінального законодавства України в цій сфері.

Для досягнення цієї мети аналізуються спричинені комп'ютеризацією та інформатизацією зміни в структурі та змісті суспільних відносин; досліджуються чинники суспільної небезпечності

комп'ютерних злочинів; з'ясовуються основні тенденції розвитку кримінального законодавства в цій сфері; проводиться ретельний аналіз змісту юридичних ознак складів злочину, передбачених розділом XVI КК України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»; формулюються основні положення, які дають можливість відмежовувати комп'ютерні злочини від суміжних; на ґрунті вивчення даних аспектів кримінальної відповідальності за досліджувані злочини пропонуються для обговорення можливі зміни до чинного кримінального законодавства про комп'ютерні злочини.

Курс складається з дев'яти тем:

1. Соціально-економічна зумовленість кримінальної відповідальності за злочини у сфері використання комп'ютерної техніки.
2. Загальна характеристика «комп'ютерних» злочинів.
3. Несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.
4. Кримінальна відповідальність за незаконні дії зі шкідливими програмними або технічними засобами.
5. Кримінально-правова охорона комп'ютерної інформації з обмеженим доступом (ст. 361-2 КК України).
6. Комп'ютерні злочини, що вчиняються особами, які наділені певними правами щодо доступу до інформації або використання ЕОМ, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку (статті 362 та 363 КК України).
7. Кримінальна відповідальність за масове розповсюдження повідомлень електрозв'язку (аналіз складу злочину, передбаченого ст. 363-1 КК України).
8. Відмежування комп'ютерних злочинів від суміжних правопорушень.
9. Напрями вдосконалення кримінального законодавства України про комп'ютерні злочини.

Опанувавши зміст курсу «Злочини у сфері використання комп'ютерної техніки», слухачі повинні:

знати:

– основні етапи розвитку національного, зарубіжного та міжнародного кримінального законодавства про комп'ютерні злочини;

– характеристику родового об'єкта злочинів у сфері використання ЕОМ, автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку;

– зміст юридичних ознак складів злочинів, передбачених розділом XVI Кримінального кодексу України;

– критерії відмежування комп'ютерних злочинів від суміжних;

– принципи кримінально-правового відображення тенденцій інформатизації суспільства та напрями вдосконалення законодавства з питань протидії комп'ютерним злочинам;

мати вміння і оволодіти практичними навичками:

– кваліфікувати злочини у сфері використання ЕОМ, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку;

– відмежовувати комп'ютерні злочини від суміжних.

Розділ 1. Соціально-економічна зумовленість кримінальної відповідальності за злочини у сфері використання комп'ютерної техніки

1.1. Інформаційний вибух, інформатизація, комп'ютеризація

Право – регулятор суспільних відносин. Тому зміни в їх структурі й змісті повинні знаходити відображення в нормах права. Істотні зміни в суспільних відносинах на сучасному етапі розвитку зумовлені науково-технічним прогресом. Упровадження новітніх технологій в усі сфери життя суспільства неминуче приводить до значного розширення інформаційних потоків, зростання інформаційної потреби (*«інформаційний вибух»*). Щоб діяти ефективно сучасній людині необхідно мати набагато більший обсяг інформації, ніж людині, яка жила, приміром, на початку XX ст.

Однак зміна кількісних характеристик інформаційних процесів спричинює певну суперечність: з одного боку, для ефективної та результативної діяльності людині потрібні зростаючі обсяги інформації, з іншого боку, фізична здатність людини до зберігання, передавання й перероблення інформації обмежена.

Подолання такої ситуації пов'язане з розвитком суспільних процесів, які отримали назву *інформатизація*. Відповідно до Закону України «Про Національну програму інформатизації» вона становить «сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки».

З процесом інформатизації тісно пов'язаний процес *комп'ютеризації* – розвиток і впровадження в різні сфери життя й діяльності людини технічної бази, яка забезпечує оперативну роботу з інформацією. Комп'ютерна техніка стала важливою умовою існування та розвитку суспільства, бо саме вона дає змогу зберігати, опрацьовувати та передавати величезні обсяги інформації, без яких нині є неможливою ефективна діяльність. Отже, комп'ютеризація як реакція людства на описану ситуацію «інформаційного вибуху» є технічною основою сучасного етапу інформатизації. А полягає вона в появі, розвитку та розширенні сфери застосування комп'ютерної техніки.

За незначний період існування комп'ютерних технологій людство здобуло в цій сфері величезних досягнень. Наведемо такі дані:

– 1945 р. в США було створено перший комп'ютер, який займав окрему будівлю, споживав 150 кВт електроенергії, що було достатньо для роботи невеликого заводу; сучасні комп'ютери вміщуються на робочому столі, важать декілька кілограмів, споживають електроенергії не більше настільної лампи;

– перші ЕОМ виконували до 1000 операцій на секунду та давали можливість зберігати в пам'яті сотні рядків тексту програм; сучасні комп'ютери мають продуктивність порядку мільярда операцій на секунду й у їх пам'яті може міститися інформація, еквівалентна тексту сотень книг. Ці показники продовжують стрімко зростати. Так, корпорація Ай-Бі-Ем у 1999 р. розповсюдила інформацію про плани щодо розроблення нового суперкомп'ютера «Блю Джин», швидкодія котрого повинна досягати одного квадрильйона операцій на секунду. Якщо за допомогою гістограми порівняти швидкодію, то сучасним комп'ютерам буде відповідати смужка довжиною 2,5 см, а «Блю Джин» – 50 км![1]

Революційні зміни мають місце і в технологіях приймання та передавання інформації. У травні 1999 р. в США відбувся офіційний пуск в експлуатацію комп'ютерної мережі INTERNET-2, що забезпечує передавання інформації зі швидкістю від 4-х до 10 гігабайта на секунду. Показовим є факт: енциклопедія «Британіка» (30 книжкових томів) пересилається через INTERNET-2 за одну секунду[2].

Спостерігається зростання кількості ЕОМ у світі: 1954 р.– близько 100 ЕОМ, 1983 р.– 2 млн ЕОМ, на сьогодні – тільки користувачів популярного ділового пакета програм Microsoft Office нараховується понад 30 млн.

---

[1] Див.: *IBM* строит суперкомпьютер // Зеркало недели.– 1999.– № 50 (271).– 18 декабря.– С. 24.

[2] Див.: *Коржс Ю.* Інтернет в Україні // Вісник НАН України.– 1999.– № 1.– С. 55.

Паралельно з розвитком комп'ютерної техніки розширюється сфера її застосування: перший комп'ютер – «ЕНІАК» – був призначений для розрахунку балістичних таблиць; сучасні комп'ютерні технології проникнули буквально у всі сфери діяльності людини. Так, у науці комп'ютери стали незамінним інструментом для вчених, за їх допомогою моделюються різні складні процеси й об'єкти. Завдяки комп'ютерним мережам стало можливим одержання будь-якої інформації з будь-якої точки планети за лічені хвилини. Використовуючи комп'ютери, медики діагностують захворювання. На переважній більшості підприємств комп'ютери керують верстатами та допомагають вести бухгалтерію. Широко застосовуються електронні системи міжбанківських платежів, з'явилися комп'ютерні гроші – кредитні картки. Комп'ютерна техніка застосовується у виробничих процесах, ефективність яких сьогодні в основному визначається не фізичними й трудовими навиками, а здатністю до творчої, розумової діяльності, пов'язаної з опрацюванням інформації, що надходить, і прийняттям рішення. Широке використання комп'ютерні технології знайшли в державних органах. Досягнення технології на сучасному етапі уможливили вживлення електронних пристроїв у людські органи[1]. Цікавим є прогноз розвитку цього процесу в XXI ст., який зробив О. А. Гаврилов: «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 й інформаційну економіку. Виникне планетарна система телекомунікації»[2].

Таким чином, розвиток комп'ютерної техніки характеризується стрімким зростанням показників швидкості роботи та збільшенням обсягів інформації, яку дають можливість опрацьовувати комп'ютери. Завдяки успіхам технології ці процеси супроводжуються зменшенням відношення ціни та продуктивності ЕОМ, що зумовлює значне розширення сфери застосування комп'ютерної техніки. Наведені ознаки і становлять зміст «комп'ютеризації».

[1] Див.: *Карамов Я.* Человек-киборг // Комсомольская правда.– 1998.– 16 октября.

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

1.2. Суспільна небезпечність комп'ютерних злочинів

Розширення сфери застосування комп'ютерних технологій, без сумніву, має позитивне значення для розвитку суспільних відносин у сфері інформатизації. Однак воно спричиняє й негативні наслідки: появу нового виду злочинів – злочинів у сфері використання ЕОМ, автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку. Відмітимо, що в Україні спостерігається значне зростання показників комп'ютерної злочинності. Так, якщо у 2000 р. «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], у 2001 р. було виявлено 7 комп'ютерних злочинів, у 2002 – 25, а у 2003 – було порушено більш ніж 120 відповідних кримінальних справ[2], то лише у першому півріччі 2008 р. було виявлено 1119 злочинів у сфері інтелектуальної власності та високих технологій, кримінальні справи по 728 злочинам даної категорії були направлені до суду[3]. Наведені дані абсолютно чітко свідчать про те, що «комп'ютерні» злочини вже перестали бути екзотикою, набули значення достатньо реальної загрози і потребують адекватних заходів протидії. Це ставить перед державою та суспільством завдання щодо розроблення засобів і методів боротьби із зазначеними злочинами та відповідно вдосконалення нормативної бази для цього.

Суспільна небезпечність злочинів у сфері використання комп'ютерної техніки зумовлена насамперед соціальною значущістю інформаційних відносин у сучасному суспільстві: їх нормаль-

[1] *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: *М. Гуцалюк*. Координація боротьби з комп'ютерною злочинністю // Право України.– 2002.– № 5.– С. 121).

[2] Див.: *Корягин А.* Преступность в сфере компьютерных и интернет-технологий: актуальность и проблемы борьбы с ней.– Режим доступа: http://www.crime-research.ru/library/Koryagin.html (Наводиться за: *Голубев В.* Организационно-правовые аспекты противодействия компьютерному терроризму // Підприємництво господарство і право.– 2004.– № 7.– С. 121).

[3] *В Украине* совершено более 1 тыс. «кибер-преступлений» за полгода // Новости сайта Центра исследования компьютерной преступности.– 09.08.2008.– Режим доступа: http://www.crime-research.ru/news/09.08.2008/4710/

не 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 порушує багато інших суспільних відносин.

Підвищена суспільна небезпечність комп'ютерних злочинів на сучасному етапі пов'язана також з істотними змінами в інформаційних відносинах, спричиненими розвитком комп'ютерної техніки. Механізм впливу технології на суспільні відносини полягає в тому, що з розвитком суспільства та постійним включенням технічних досягнень у систему діяльності людини вона все більше технологізується. Технологія стає важливою частиною найрізноманітніших відносин, зумовлює істотні зміни в суспільстві[1]. Наприклад, розвиток аграрно-ремісничих технологій стимулював появу первинних форм держави, якісну зміну права та форм власності, сприяв утворенню міст. Промислове виробництво й індустріальні технології привели до формування держав нового типу, зміни соціальної структури суспільства, зростання міського населення[2].

У свою чергу комп'ютерна технологія, яка виникла внаслідок зміни кількісних характеристик інформаційних процесів (збільшення обсягів інформації, що використовується, передається, зберігається і т. ін.), сприяла *якісній зміні* інформаційних суспільних відносин. Ці зміни відбилися в тому, що інформаційні зв'язки й інформація стали розглядатися в новій системі координат – як економічні категорії. Інформація стає цінним продуктом і основним товаром[3]. 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 найважливіших видів ресурсів, які визначають економічну, політичну та (або) військову міць їх власника[4].

[1] Див.: *Ракитов А. И.* Философия компьютерной революции.– М.: Политиздат, 1991.– С. 16.

[2] Див.: *Бачинин В. А.* Философия права и преступления.– Х.: Фолио, 1999.– С. 78.

[3] Див.: *Философия:* Учебник для высших учебных заведений.– Ростов н/Д: Феникс, 1995.– С. 535.

[4] Див.: *Воройский Ф. С.* Систематизированный толковый словарь по информатике (Вводный курс по информатике и вычислительной технике в терминах).– М.: Киберия, 1998.– С. 16.

Зростання значущості інформації, процесів, пов'язаних з її виробництвом, зумовило певні зміни в структурі суспільного виробництва. Так, ще наприкінці 30-х років XX ст. деякими економістами було запропоновано розглядати суспільне виробництво як сукупність трьох основних секторів: первинного, до якого відносяться видобувні галузі й сільське господарство; вторинного, що включає обробну промисловість, і третинного – сфери послуг[1]. Нині 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.

Отже, ще одним показником підвищеної суспільної небезпечності злочинів у сфері використання комп'ютерної техніки є зростаюча економічна цінність предмета цих злочинів – комп'ютерної інформації. На думку експертів Організації з Безпеки та Співробітництва в Європі (ОБСЄ) злочинність, пов'язана з використанням комп'ютерних систем та мереж, здатна створити не менший хаос ніж теперішня економічна криза. Шкода, яка щорічно заподіюється кіберзлочинністю у світі, оцінюється приблизно у 100 млрд доларів США і має тенденцію до зростання[2]. Також фахівці відзначають, що ці злочини набувають міжнародного характеру та загрожують економічним основам держав і світовій економічній системі[3].

Слід відзначити, що небезпека досліджуваних злочинів багаторазово збільшується, коли злочинець отримує доступ до автоматизованих систем, які використовуються в національній обороні[4], керуванні рухом повітряного або наземного транспорту, контролі над небезпечним виробництвом та інших сферах людської діяльності, які становлять підвищену небезпеку. У таких випадках неза-

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

[2] *Киберпреступность* страшнее финансового кризиса // Новости сайта Центра исследования компьютерной преступности.– 03.12.2008.– Режим доступа: http://www.crime-research.ru/news/03.12.2008/5056/

[3] Див.: *Антонов С.* Компьютерные преступления в банковской сфере // Юридическая практика.– 1997.– № 8.– С. 7.

[4] Див.: *Фролов В. С.* «Думающее» оружие.– М.: Знание, 1991. (Новое в жизни, науке и технике.– Сер. Радиоэлектроника и связь, № 7).– С. 58–62.

конне втручання може не тільки призвести до значних матеріальних втрат, але й спричинити людські жертви.

Зазначимо, що силові відомства Росії та США визнають комп'ютерні злочини як реальну загрозу безпеці країни. Так, у ФСБ РФ заявляють про те, що у найближчому майбутньому існує небезпека терористичних кібератак на інформаційні мережі державних структур та приватних компаній, пов'язаних з керуванням об'єктами антикризової інфраструктури[1]. У свою чергу, аналітичний звіт американських фахівців «Оцінка загроз національній безпеці 2008–2013» містить дані про те, що загроза кібертероризму в найближчі п'ять років збільшуватиметься[2]. Відповідну оцінку цим негативним явищам дає і національний законодавець. Закон України «Про основи національної безпеки України» від 19 червня 2003 р. до загроз національній безпеці в інформаційній сфері відносить, зокрема, комп'ютерну злочинність та комп'ютерний тероризм.

Стійка тенденція зростання суспільної небезпечності комп'ютерних злочинів зумовлена також і прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

Викладене дає можливість визначити такі показники суспільної небезпечності злочинів у сфері використання електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку:

1) досліджувані злочини, завдаючи шкоди розвиткові інформаційних відносин, зашкоджують великій кількості інших соціально значущих суспільних відносин;

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

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.

---

[1] *Кибератака* на информационные сети государственных структур // Новости сайта Центра исследования компьютерной преступности.– 16.04.2009.– Режим доступа: http://www.crime-research.ru/news/16.04.2009/5797/

[2] *Угроза* кибертерроризма будет только возрастать // Новости сайта Центра исследования компьютерной преступности.– 27.12.2008.– Режим доступа: http://www.crime-research.ru/news/27.12.2008/5106/

1.3. Основні тенденції розвитку кримінального законодавства про комп'ютерні злочини

В Україні комп'ютерні технології впроваджуються з істотним відставанням у часі й масштабах від передових західних країн і дефіцит практики позначається на темпах формування законодавства. 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.

У країнах Західної Європи законодавець з питання злочинів у сфері використання комп'ютерних технологій обрав два напрями:

По-перше, багато статей про посягання на особу, власність і т. ін. було доповнено нормами про відповідальність за ці злочини у випадках їх скоєння з використанням комп'ютерної техніки.

По-друге, до Кримінального кодексу (далі – КК) було внесено нові норми про відповідальність за посягання на якісно новий об'єкт, що й зумовило виникнення злочинів у сфері використання ЕОМ, автоматизованих систем і комп'ютерних мереж.

Як приклад достатньо розглянути відображення цих двох напрямів 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, установленого порядку обігу документів, проти національної безпеки, інтелектуальної власності, комерційної таємниці.

Так, наприклад, розділ 15 КК ФРН[1] «Порушення недоторканності і таємниці приватного життя» – доповнено ст. 202а «Дії, спрямовані на одержання відомостей», в 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 ст. 263а «Комп'ютерне шахрайство», яка перед-

---

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

бачає 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 ст. 226-15 установлено 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 посягання на основоположні інтереси нації; за збирання і 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 передбачено норми про відповідальність за посягання на відносини у сфері використання ЕОМ, автоматизованих 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 об'єднано 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 тех-

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

нікою, 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 ЕОМ, автоматизованих систем і комп'ютерних мереж було приділено й на міжнародному рівні. У цьому плані видаються цікавими рекомендації Ради Європи щодо вдосконалення законодавства про комп'ютерні злочини.

13 вересня 1989 р. Радою Європи було прийнято рекомендації, розроблені Комітетом експертів з комп'ютерних злочинів Союзу Європи. Даний документ містить два списки дій – мінімальний і додатковий. У мінімальний список включено 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 передбачено діяння, криміналізовані в окремих державах, але з приводу криміналізації яких усіма державами, що входять у Союз Європи, згоди досягнуто не було. Мінімальний список: комп'ютерне шахрайство[1], 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. Додатковий список становлять такі дії: зміна комп'ютерних даних або програм, комп'ютерне шпигунство, несанкціоноване використання комп'ютерів, несанкціоноване використання захищених комп'ютерних програм[2].

Одним із основних міжнародних нормативних документів у цій сфері є Конвенція про кіберзлочинність, прийнята в рамках Ради Європи 23 листопада 2001 р., з Додатковим протоколом, який стосу-

[1] Слід відзначити, що використання європейськими фахівцями терміна «шахрайство» (fraud) у контексті комп'ютерних злочинів, видається не зовсім вдалим, тому що це вимагає визнання як істинних висловлювань типу «обман комп'ютера» або «зловживання довірою комп'ютера».

[2] *Наводиться* за 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

ється криміналізації дій расистського та ксенофобського характеру, вчинених через комп'ютерні системи. У вересні 2005 р. цю конвенцію було ратифіковано Верховною Радою України[1].

Діяння, які мають бути криміналізовані країнами-учасницями, поділяються Конвенцією на чотири групи: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ; нелегальне перехоплення; втручання в дані; втручання в систему; зловживання пристроями); 2) правопорушення, пов'язані з комп'ютерами (підроблення, пов'язане з комп'ютерами, шахрайство, пов'язане з комп'ютерами); 3) правопорушення, пов'язані зі змістом інформації (вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем; пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем; розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем; набуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи; володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації); 4) правопорушення авторських і суміжних прав.

Отже, перші рекомендації Ради Європи більшою мірою відповідають американському підходу до вирішення проблеми комп'ютерних злочинів. Це можна пояснити тим, що в США вперше у світі комп'ютерна техніка набула значного поширення, там само вперше було поставлено питання про комп'ютерні злочини, а рішення Ради Європи 1989 р. є запозиченням цього рішення без оцінки специфіки систематизації континентального законодавства. Однак уже в Конвенції про кіберзлочинність ми виявляємо відповідну континентальним правовим традиціям класифікацію злочинів, пов'язаних із комп'ютерною технікою. У ній вирізняється група злочинів з якісно новим об'єктом (порушення конфіденційності, цілісності та придатності комп'ютерних даних і систем) й визначаються злочинні посягання на традиційні об'єкти, що скоюються з використанням комп'ютерної техніки.

Проблема цих злочинів привернула серйозну увагу і вчених. З'явилися праці, в яких робиться спроба розкрити сутність і юридичні ознаки злочинів у сфері використання комп'ютерних технологій. Особливо активізувалася ця робота в період підготування

[1] Див.: *Закон* України «Про ратифікацію Конвенції про кіберзлочинність» від 7 вересня 2005 р.

проектів КК України та Росії. Не можна не відзначити, що питання з розв'язання цієї проблеми, зокрема з визначення поняття цих злочинів, їх місця в системі КК, вирішувалися по-різному.

Аналіз пропозицій щодо вдосконалення кримінального законодавства про злочини у сфері використання комп'ютерної техніки дає можливість 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 р. А. В. Черних[2] до розгляданих злочинів включав 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 А. 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 авторського права на програмне забезпечення). М. Вертузаєв і А. Попов[6] пропонували віднести до них: використання комп'ютера для аналізу та моделювання злочинних дій; злочини, пов'язані з ком-

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

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

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

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

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

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

п'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 було враховано 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 і комп'ютерних мереж» (див. дод. 1). Необхідно також зауважити, що вдосконалення кримінального законодавства про відповідальність за комп'ютерні злочини триває, двічі положення згаданого розділу змінювалися та доповнювалися (Закони України «Про внесення змін до Кримінального кодексу України щодо відповідальності за незаконне втручання в роботу мереж електрозв'язку» від 5 червня 2003 р. та «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» від 23 грудня 2004 р.).

Запитання для самоконтролю та самоперевірки

1. Що таке «інформаційний вибух»?
2. Чим комп'ютеризація відрізняється від інформатизації?
3. У чому специфіка впливу розвитку інформаційних технологій на суспільні відносини?
4. Охарактеризуйте основні чинники суспільної небезпечності комп'ютерних злочинів.
5. Назвіть головні тенденції розвитку зарубіжного та міжнародного законодавства про комп'ютерні злочини.

Розділ 2. Загальна характеристика комп'ютерних злочинів

2.1. Родовий об'єкт комп'ютерних злочинів

Досліджуючи родовий об'єкт злочинів у сфері використання ЕОМ, автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку, насамперед цікаво порівняти КК України 1960 р. і 2001 р. щодо питання про місце цих злочинів у системі Особливої частини.

Стаття 198[1] «Порушення роботи автоматизованих систем» КК 1960 р. була розташована в главі IX «Злочини проти порядку управління». Отже, родовим об'єктом злочину, передбаченого цією статтею, був установлений 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,– установлений порядок використання автоматизованої системи як матеріального носія управлінської діяльності. Таке законодавче рішення не відповідало цілям кримінально-правової охорони суспільних відносин у сфері використання ЕОМ, автоматизованих систем і комп'ютерних мереж, 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.

---

[1] *Кримінальне* право України. Особлива частина: Підручник для студентів юрид. 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.– С. 638.

Цього недоліку позбавлений КК України 2001 р. Об'єднавши в одному розділі норми про відповідальність за злочини у сфері використання ЕОМ, систем і комп'ютерних мереж, він повніше відбиває соціальну значущість відносин інформатизації життя суспільства, що постійно розвивається.

Родовий об'єкт злочинів у сфері використання ЕОМ, систем і комп'ютерних мереж у кримінальному праві України досліджений недостатньо. Основна причина полягає насамперед у новизні норм, які передбачають відповідальність за ці злочини. Тому 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 р., коли було прийнято КК Російської Федерації, який передбачив у главі 28 злочини у сфері комп'ютерної інформації.

Аналіз визначень, які пропонувалися російськими криміналістами, дає змогу зробити висновок про те, що єдиної точки зору на сутність родового об'єкта злочинів у сфері використання ЕОМ, систем і комп'ютерних мереж не було. Одні автори вважали, що ці злочини «спрямовані проти тієї частини встановленого порядку суспільних відносин, яка регулює 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 ЕОМ, систем і комп'ютерних мереж є посяганням на системи опрацювання даних. Так, автори підручника під редакцією Б. В. Здравомислова родовим об'єктом цих злочинів визначають «права та інтереси фізичних і юридичних осіб, суспільства і 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[1]. Найбільш повно цю позицію відображено в Коментарі 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»[2].

Така позиція фактично залишилася незмінною і в літературі, виданій у 2000–2001 рр. Так, К. С. Скоромніков визначає досліджуваний родовий об'єкт як «суспільні відносини, що виникають у процесі комп'ютерного опрацювання інформації»[3]. Це дає можливість сказати, що серед російських учених таке визначення родового об'єкта злочинів у сфері використання ЕОМ, систем і комп'ютерних мереж є найбільш визнаним.

Втім видається, що визначення безпеки автоматизованих систем опрацювання даних як родового об'єкта цих злочинів не відбиває його 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, котрі 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 у сфері використання ЕОМ, систем і 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

---

[1] Див.: *Комментарий* к Уголовному кодексу Российской Федерации / Отв. ред. докт. юрид. наук, проф. А. В. Наумов.– М.: Юристъ,– 1996.– С. 662.

[2] Див.: *Комментарий* к Уголовному кодексу Российской Федерации.– 2-е изд., изм. и доп. / Под общ. ред. Ю. И. Скуратова и В. М. Лебедева.– М.: Издательская группа Норма-Инфра-М, 1998.– С. 634.

[3] Див.: *Уголовное* право России. Особенная часть: Учебник / Отв. ред. докт. юрид. наук, проф. Б. В. Здравомыслов.– М.: Юристъ, 1996.– С. 350.

[1] Див.: *Уголовное* Право. Особенная часть: Учебник / Под ред. проф. А. И. Рарога.– М.: Ин-т международного права и экономики. Изд-во «Триада, Лтд», 1997.– С. 147.

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

[3] Див.: *Скоромников К. С.* Компьютерное право Российской Федерации.– М.: Изд-во МНЭПУ, 2000.– С. 178.

інших відносин, а отже, кримінально-правову заборону на їх порушення. Це положення прямо стосується питання про зміст родового об'єкта досліджуваних злочинів. Як уже було відзначено, специфікою розвитку сучасного суспільства є ускладнення людської діяльності, зростання інформаційних потреб, загальна комп'ютеризація та інформатизація.

Усе це закономірно зумовлює розвиток певної групи однорідних суспільних відносин, які йменуються *інформаційними*. Ці 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 зазначити, що поняття «інформаційні відносини» зазнало серйозних змін, обумовлених самим розвитком процесу інформатизації суспільства. Так, якщо наприкінці 70-х років А. Б. Венгеров визначав їх як «відносини, які складаються у сфері управління народним господарством між працівниками, їх колективами в процесі реєстрації, збирання, передавання й опрацювання інформації»[2], то вже в 1992 р. Закон України «Про інформацію» визначає їх як «відносини, які виникають у всіх сферах життя і діяльності суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації». 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.

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

Зміст інформаційних відносин становлять 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 в будь-якій формі з використанням будь-яких засобів, але в межах чинного законодавства.

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

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

До основних обов'язків суб'єктів інформаційних відносин відносяться такі: поважати інформаційні права інших суб'єктів; використовувати інформацію згідно із законом або договором (угодою); забезпечувати доступ до інформації всім споживачам на умовах, передбачених законом або угодою; зберігати інформацію в належному стані протягом установленого 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, котрий є відтворенням в іншій формі особливостей першої системи в особливостях другої[1]. Деяка подія породжує ланцюг змін матеріальних об'єктів, що спричинено 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, перетворення, зберігання та передавання інформації відбуваються за допомогою матеріальних об'єктів (носіїв інформації), стани яких і слугують сигналами. При цьому необхідно, щоб об'єкт, який відображається, і об'єкт, який відображає, були в такій взаємодії, за якої зміна стану одного з них приводила б до зміни стану другого. Важливо зазначити 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, а властивість співвідношення, зв'язку між об'єктами, стан одного з яких є сигналом стану іншого[2]. Кібернетикою носій інфор-

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

[2] Див.: *Тарасенко Ф. П.* К определению понятия «информация» в кибернетике // Вопросы философии.– 1963.– № 4.– С. 83–84.

мації визначається як «матеріал (речовина) для запису, зберігання та подальшого відтворення інформації»[1].

Таким чином, співвідношення понять «інформація» і «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»[2]. 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» та «адресність». При цьому код є характером 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 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 істотним є те, що соціально значущим у сфері правового регулювання суспільних відносин з приводу інформації буде не просте володіння носієм інформації, але й наявність можливості «витягти» з нього інформацію.

Важливою характеристикою інформаційних відносин є їхня *соціальна значущість:* 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 опосередковує зв'язки людини з людиною, людини з природою і технікою. Досить чітко соціальну значущість інформаційних відносин сформулював засновник кібернетики Норберт Вінер: «...будь-який організм скріплюється наявністю засобів придбання, використання, зберігання та передавання інформації»[1]. *Інформаційні суспільні відносини і є засобом для одержання, зберігання та передавання інформації.* Тому вони як основа результативної, ефективної діяльності конкретної людини врешті-решт є необхідною умовою розвитку та стабільності суспільства.

[1] Див.: *Словарь* по кибернетике / Под ред. акад. В. М. Глушкова.– К.: Главная редакция Украинской Советской энциклопедии, 1979.– С. 353.

[2] Див.: *Клаус Г.* Кибернетика и общество.– М., 1967.– С. 37. (Наводиться за: *Батурин Ю. М.* Проблемы компьютерного права.– М.: Юридическая литература, 1991.– С. 16).

Істотною 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 ресурсом, який, за показником економічної ефективності, відіграватиме домінуючу роль, витіснивши на другий план сировину й енергію[2].

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

Юридичною підставою для цього є ст. 34 Конституції України, яка гарантує право кожного вільно збирати, зберігати, використовувати та розповсюджувати інформацію, щодо якої немає обмежень, установлених законом, а також Закон України «Про інформацію» від 2 жовтня 1992 р., котрий визначив поняття інформації, інформаційних відносин, зміст об'єктів цих відносин, права й обов'язки їх учасників. У ньому зазначено основні принципи та напрями державної інформаційної політики; визначено інформаційну діяльність, її напрями та види. Також законом закріплено 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 є 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 і мереж електрозв'язку», є тільки частина інформаційних відносин, які можна визначити як *інформаційні відносини, засобом забезпечення яких є ЕОМ, системи, комп'ютерні мережі та мережі електрозв'язку.* Інакше кажучи, злочини, передбачені цим розділом, посягають

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

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

на *певну частину* інформаційних відносин – інформаційні відносини, пов'язані із застосуванням спеціальних технічних засобів. У кримінальному законі наводяться три види таких засобів:

1) електронно-обчислювальна машина (комп'ютер) – функціональний пристрій, що складається з одного або декількох взаємопов'язаних центральних процесорів і периферійних пристроїв і може виконувати розрахунки без участі людини[1];

2) автоматизована система – організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей і персоналу, що здійснює цю діяльність[2];

3) 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];

4) телекомунікаційна мережа (мережа електрозв'язку) – комплекс технічних засобів телекомунікацій і споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого роду за допомогою радіо, проводових, оптичних чи інших електромагнітних систем між кінцевим обладнанням[4].

Залежно від цих засобів інформаційні відносини, які є родовим об'єктом досліджуваних злочинів, можуть бути поділені на чотири види:

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

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

в) інформаційні відносини, засобом забезпечення яких є комп'ютерні мережі;

г) інформаційні відносини, засобом забезпечення яких є мережі електрозв'язку.

---

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

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

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

[4] Див.: Стаття 1 Закону України «Про телекомунікації» від 18 листопада 2003 року.

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. Зазначимо, що під ЕОМ розуміються не тільки комп'ютери в їх «класичному», можна сказати звичному, вигляді, тобто «системний блок – монітор – клавіатура – принтер», але й інше устаткування, яке містить процесор і може виконувати розрахунки без участі людини. Так, у практиці російських правоохоронних органів мали місце випадки знищення інформації, яка зберігалася в пам'яті електронних касових апаратів. У результаті такого втручання знищувалася або модифікувалася інформація щодо платежів, які надійшли до каси, що в подальшому дозволяло приховувати реальні доходи від податкових органів[1]. Вчинене, безсумнівно, є ухиленням від сплати податків, але крім цього подібні дії необхідно додатково кваліфікувати як втручання в роботу ЕОМ, що призвело до знищення або перекручення комп'ютерної інформації. Адже касовий апарат містить процесор і може виконувати розрахунки без участі людини, тобто є ЕОМ за визначенням. Те саме стосується й мобільних телефонів. Тому випадки так званого «перепрошивання» мобільних телефонів, незаконної зміни їх IMEI-кодів слід також кваліфікувати як несанкціоноване втручання в роботу ЕОМ, що призвело до підроблення комп'ютерної інформації.

Використання комп'ютерних систем відноситься до більш складних інформаційних відносин. Слід зазначити, що аналіз нормативно-правових актів показує невідповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31 травня 2005 р. (цей закон змінив Закон України «Про захист інформації в автоматизованих системах» від 5 липня 1994 р.) та ДСТУ 2226-93 «Автоматизовані системи. Терміни та визначення» від 1 липня 1994 р. Термін «автоматизована система» визначається в цих нормативних актах неоднаково.

Так, відповідно до закону інформаційна (автоматизована) система – це «організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і про-

---

[1] Див.: *Сайтарлы Т.* Компьютерная преступность бьет по налогам.– Режим доступа: http://www.crime-research.ru/news/10.08.2004/1336

грамних засобів». Названий стандарт визначає автоматизовану систему 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, неможливо відмежувати автоматизовану систему від ЕОМ, оскільки вона теж призначена для опрацювання даних, до її складу входять процесор, контролери, накопичувачі інформації (засоби обчислювальної техніки та зв'язку), її необхідним елементом є програмне забезпечення.

У свою чергу, визначення, яке міститься в стандарті, є досить чітким і характеризує призначення автоматизованої системи – автоматизація певного виду людської діяльності. Визначення автоматизованої системи, виходячи з її призначення, видається більш вдалим для використання в контексті кримінально-правового дослідження, тому що дає можливість правильно вирішувати питання про соціальну значущість інформаційних відносин, пов'язаних з автоматизованими системами, а відтак, і про суспільну небезпечність посягань на ці відносини. Автоматизовані системи використовуються для виконання широкого кола завдань, а саме: управління підприємством, технологічне підготування виробництва, контроль і випробування промислової продукції, управління службами життєзабезпечення підприємства і т. ін. 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 заподіянні шкоди інформаційним відносинам у сфері розроблення продукції та, по-друге, у загрозі заподіяння шкоди відносинам, що забезпечують випуск доброякісної продукції.

Третій вид інформаційних відносин, які утворюють досліджуваний родовий об'єкт, пов'язаний із використанням комп'ютерних

[1] Див.: ДСТУ 226-93. Автоматизовані системи. Терміни та визначення.– 01.07.94.– С. 2.

[2] Там само.– С. 12.

мереж, що 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 Інтернет, що застосовується в основному для таких видів роботи з інформацією, як: електронна пошта; передавання файлів; віддалений доступ – можливість підключатися до віддаленого комп'ютера й працювати з ним в інтерактивному режимі[1]. 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 розвитку комп'ютерних мереж в Україні сьогодні приділяється велика увага. Про це, зокрема, свідчить прийняття спеціальних нормативно-правових актів, одним із яких є Указ Президента України від 31 липня 2000 р. «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет і забезпечення широкого доступу до цієї мережі в Україні»[2], який передбачає заходи, спрямовані на розширення застосування мережі Інтернет в Україні.

Інформаційні відносини, засобом забезпечення яких є мережі електрозв'язку, полягають у наданні й отриманні послуг електричного зв'язку, тобто у використанні мереж електрозв'язку для передачі або прийому інформації. Стосовно до визначення змісту цих суспільних відносин певний інтерес становить питання їх відмежування від інформаційних відносин, засобом забезпечення яких є комп'ютерні мережі. Закон України «Про телекомунікації» від 18 листопада 2005 р. містить таке поняття, як «інформаційна система загального доступу», яке визначається таким чином: «сукупність телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та передавання даних». Дані, відповідно до закону,– це інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки.

Отже, можна дійти висновку, що комп'ютерні мережі, тобто технічні засоби, за допомогою яких здійснюється опрацювання

[1] Див.: *Глистер Пол.* Новый Навигатор Internet.– К.: Диалектика, 1996.– С. 30–31.

[2] Див.: *Указ* Президента України від 31 липня 2000 р. № 928 «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет і забезпечення широкого доступу до цієї мережі в Україні» // Офіційний Вісник України.– 2000.– № 31.– Ст. 1300.

й передавання комп'ютерної інформації, відносяться до телекомунікаційних мереж, а інформаційні відносини, засобом забезпечення яких є комп'ютерні мережі,– це певна частка інформаційних суспільних відносин, пов'язаних із використанням мереж електрозв'язку. Зазначимо, що таке розуміння є правильним, ураховує сучасні тенденції розвитку комп'ютерних технологій. У найближчому майбутньому нас очікує ситуація, коли для зв'язку будуть використовуватися виключно комп'ютерні мережі (мережі, що забезпечують зв'язок між комп'ютерами). Уже зараз ми маємо мобільний зв'язок, цифрові АТС тощо.

Отже, наявність у назві розділу XVI КК України та диспозиціях статей цього розділу терміна «мережа електрозв'язку» (відповідно до згаданого закону «телекомунікаційна мережа») можна визначити як відображення сучасних тенденцій розвитку технологій зв'язку. Однак наявність у законі про кримінальну відповідальність одночасно з цим терміном іншого – «комп'ютерна мережа» – фактично приводить до того, що під мережею електрозв'язку треба розуміти всі телекомунікаційні мережі, крім комп'ютерних (мережі міського, міжміського та міжнародного телефонного зв'язку, рухомого (мобільного) зв'язку, проводового радіомовлення, ефірного телерадіомовлення тощо). Таким чином, під інформаційними відносинами, засобом забезпечення яких є мережі електрозв'язку, слід розуміти суспільні відносини у сфері використання телекомунікаційних мереж за винятком комп'ютерних мереж.

2.2. Визначення поняття «комп'ютерний злочин»

Із визначенням родового об'єкта злочинів у сфері використання ЕОМ, систем, комп'ютерних мереж і мереж електрозв'язку 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 і мереж електрозв'язку». У літературі все частіше використовується таке їх визначення, як «комп'ютерні злочини» з огляду на специфіку їхнього предмета.

Слід підкреслити, що це питання є актуальним, оскільки в найменуванні злочинів, поєднаних родовим об'єктом, повинна відбиватися їхня сутність, основний зміст, що дало б змогу відмежовувати їх від інших та забезпечити правильну кваліфікацію. Відсутність чіткого визначення злочинів, передбачених у розділі XVI КК України, також значно ускладнює діяльність правоохоронних органів щодо боротьби з ними. Проведений нами аналіз звітних документів УМВС у різних областях свідчить про те, що досить часто до злочинів у сфері використання ЕОМ, систем і 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 й предмета досліджуваних злочинів, правомірно об'єднати злочини, які посягають на інформаційні відносини у сфері використання ЕОМ, систем, комп'ютерних мереж і мереж електрозв'язку, 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» трапляється доволі 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, деякі автори вважають, що до комп'ютерної злочинності відносяться всі протизаконні дії, за яких електронне опрацювання інформації є знаряддям їх вчинення і (чи) засобом[2], або всі протизаконні діяння, предметом і засобом здійснення яких є процедури й методи, а також процес комп'ютерного опрацювання

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

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

даних[1]. Пропонується і таке визначення комп'ютерних злочинів: «усі протизаконні дії, при яких електронне опрацювання інформації було засобом їх вчинення або їх об'єктом»[2]. 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»[3]. А. Н. Караханьян під комп'ютерними злочинами розуміє протизаконні дії, об'єктом або знаряддям вчинення яких є ЕОМ[4]. В. О. Голубєв уважає, що основна класифікуюча ознака належності злочинів до розряду комп'ютерних – це «використання засобів комп'ютерної техніки»[5]. В. Лісовий визначає цю ознаку інакше – «електронна обробка інформації» – незалежно від того, на якій стадії злочину вона застосовувалася[6]. Пропонується і таке визначення комп'ютерних злочинів, як: «передбачені кримінальним законом суспільно небезпечні діяння, у яких машинна інформація є або засобом, або об'єктом злочинного посягання»[7].

Деякі автори дають більш широке визначення. Так, П. Д. Біленчук і М. А. Зубань уважають, 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»[8].

---

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

[2] Див.: *Біленчук П. Д., Романюк Б. В., Цимбалюк В. С.* та ін. Комп'ютерна злочинність: Навчальний посібник.– К.: Атіка, 2002.– С. 65.

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

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

[5] Див.: *Голубєв В. О.* Правові проблеми захисту інформаційних технологій // Вісник Запорізького юридичного інституту.– 1997.– № 2.– С. 39–40.

[6] Див.: *Лісовий В.* «Комп'ютерні» злочини: питання кваліфікації // Право України.– 2002.– № 2.– С. 87.

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

[8] *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.

Згідно з таким розумінням комп'ютерної злочинності комп'ютерним злочином може визнаватися будь-який злочин (розкрадання, шпигунство, незаконне збирання відомостей, які становлять комерційну таємницю, та ін.), якщо він вчиняється з використанням комп'ютера. Видається, що таке розуміння комп'ютерних злочинів є неправильним, таким, що не дає можливість відбити їх сутність, специфіку та відрізнити від інших злочинів, в 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 значні державні таємниці, доводяться до банкрутства 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 та В. В. Пивоварова, висловлена ними ще під час обговорення проекту КК України, про внесення до переліку обставин, які 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 принтерів, незважаючи 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 України 2001 р.), так само як і ті, хто використовував для підроблення фототехніку або звичайні олівці, фарби та лезо бритви. Комп'ютерна техніка дає змогу довести до досконалості процес виготовлення підроблених докумен-

---

[1] Див.: *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.

тів (перенесені з оригіналу печатки, підписи, інші реквізити практично ідентичні). Для встановлення підробки необхідною є висококваліфікована криміналістична експертиза, але це не означає, що такого роду підроблення документів 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 змінюють 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.

Це 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 вважає, що правильніше було б говорити лише про комп'ютерні аспекти злочинів, не виділяючи їх в окрему групу[1].

Аналізуючи це питання, слід перш за все розмежувати терміни «комп'ютерні злочини» та «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[2]. Вочевидь, що остання група більш широка. Саме вона включає діяння, в яких комп'ютер є предметом, знаряддям або засобом скоєння злочину. Виокремлення цієї групи має значення для криміналістики в плані специфіки методики розслідування. Проте в кримінальному праві такий поділ видається помилковим.

Комп'ютерні злочини є новим видом суспільно небезпечних діянь і визначення їх необхідно давати з урахуванням ознаки, яка є основою чинної класифікації злочинів. Як відомо, класифікація – це розподіл предметів будь-якого роду на взаємопов'язані класи згідно з найістотнішими ознаками, властивими предметам даного роду. Як слушно зазначає М. В. Салтевський, «у кримінальному

[1] Див.: *Батурин Ю. М.* Проблемы компьютерного права.– М.: Юридическая литература, 1991.– С. 129.

[2] Див.: *Вехов В. В.* Компьютерные преступления: способы совершения и раскрытия / Под ред. акад. Б. П. Смагоринского.– М.: Право и Закон, 1996.– С. 23–24.

праві та криміналістиці вид злочину називають не за засобом (знаряддям) вчинення злочину, а за видом злочинної діяльності»[1]. Найважливішою ознакою злочинів є їх об'єкт. Класифікація за родовим об'єктом – це системоутворюючий фактор сукупності норм Особливої частини КК. Тому визначення комп'ютерних злочинів має конструюватися на основі специфічних ознак їх родового об'єкта.

Визначивши суспільні відносини, яким завдається шкода в результаті вчинення комп'ютерних злочинів, можна сформулювати й саме поняття «комп'ютерні злочини», як ***суспільно небезпечні, протиправні, кримінально карані, винні діяння, які завдають шкоди інформаційним відносинам, засобом забезпечення нормального функціонування яких є електронно-обчислювальні машини, автоматизовані системи, комп'ютерні мережі або мережі електрозв'язку.***

2.3. Кваліфікуючі ознаки комп'ютерних злочинів

Загальна характеристика комп'ютерних злочинів була б неповною без дослідження кваліфікуючих ознак цих посягань. Статті 361–362 та 363-1 КК України містять такі спільні кваліфікуючі ознаки:

1) вчинення комп'ютерного злочину повторно;

2) вчинення комп'ютерного злочину за попередньою змовою групою осіб;

3) вчинення комп'ютерного злочину, який заподіяв значну шкоду.

Оскільки в розділі XVI Особливої частини КК України не передбачено повторності однорідних злочинів, комп'ютерний злочин слід вважати вчиненим ***повторно*** у випадках, коли особа два або більше рази вчинила злочин, який було кваліфіковано за однією статтею даного розділу. При цьому вчинення декількох таких злочинів не охоплювалося єдиним умислом (злочин не був продовжуваним), особа не звільнялася від кримінальної відповідальності за

[1] *Салтевський М. В.* Основи методики розслідування злочинів, скоєних з використанням ЕОМ: Навчальний посібник.– Х.: Нац. юрид. акад. України, 2000.– С. 4.

тотожний злочин, не закінчилися строки давності притягнення до кримінальної відповідальності за раніше вчинений злочин або судимість за нього не було погашено чи знято.

Комп'ютерний злочин буде вважатися вчиненим ***групою осіб за попередньою змовою*** за наявності відповідних об'єктивних і суб'єктивних ознак. Об'єктивна сторона його може бути такою:

– діяння вчиняється двома або більше виконавцями, кожен із яких виконує всі дії, що утворюють об'єктивну сторону складу (наприклад, декілька осіб здійснюють несанкціоноване втручання з окремих терміналів і знищують певну інформацію);

– злочин вчиняється двома або більше співвиконавцями, кожен із яких виконує частину дій, що характеризують об'єктивну сторону (наприклад, одна особа вчиняє несанкціоноване втручання й перекручує комп'ютерну інформацію про користувачів комп'ютерної мережі та паролі їх доступу, а інша знищує комп'ютерну інформацію);

– злочин вчиняється двома або більше особами, при цьому лише одна з них відіграє роль виконавця, а інші є підбурювачами, пособниками або організаторами (наприклад, одна особа забезпечує іншу необхідним устаткуванням, а остання вчиняє розповсюдження шкідливої комп'ютерної програми).

При цьому кожен із співвиконавців повинен мати всі ознаки суб'єкта, тобто бути фізичною, осудною особою та досягти віку кримінальної відповідальності[1]. У випадку, коли особа не була поінформована про те, що вчиняє комп'ютерний злочин разом із малолітнім або неосудним, її дії слід кваліфікувати за правилами фактичної помилки як замах на вчинення комп'ютерного злочину 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 причинового зв'язку між діями співучасників і злочином, який вчинив виконавець.

Певну специфіку має суб'єктивна сторона комп'ютерного злочину в разі його вчинення 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 Інтернет кількома особами було вчинено розкрадання, причому ці суб'єкти один одного особисто навіть не бачили, оскільки спілкувалися за допомогою електронної мережі, в якій кожен мав свій псевдонім[1].

На прикладі конкретного злочину проілюструємо можливий розподіл ролей для вчинення комп'ютерного злочину. Щоб одержати контракт на розроблення нового обладнання, К., який займається підприємництвом у сфері високих технологій, вирішив знищити комп'ютерну інформацію про нові розробки в комп'ютерній мережі 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 несанкціоноване 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.

Значною шкодою в статтях 361–363-1 КК, якщо вона полягає в заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів (примітка до ст. 361 КК). Зазвичай ця шкода полягає в заподіянні *позитивних матеріальних збитків*. У такому випадку її необхідно оцінювати, виходячи з витрат власника на придбання комп'ютерної інформації. Але стосовно значної шкоди як кваліфікуючої ознаки комп'ютерного злочину слід зауважити, що іноді вона може виражатися і в *упущеній вигоді*. Це пояснюється тим, що на сучасному етапі будь-яка діяльність як необхідний елемент

[1] Певну специфіку матиме вчинення групою осіб за попередньою змовою злочину, передбаченого ст. 362 КК, адже суб'єкт цього злочину – спеціальний. У цьому випадку слід керуватися правилами кваліфікації співучасті зі спеціальним суб'єктом.

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

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, яка може полягати в укладанні невигідних договорів, падінні авторитету, невиконанні умов договорів тощо.

На підтвердження висновку про необхідність включення в розмір значної 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, яка через два тижні після його звільнення знищила комп'ютерну інформацію, що стосувалася новітніх розробок компанії. Збитки від втрачених контрактів і вартість відновлення знищеної інформації становили 10 млн доларів[2].

Крім матеріальної шкоди, суспільно небезпечні наслідки при вчиненні комп'ютерного злочину можуть виражатись і в *нематеріальних видах шкоди*, що зумовлено використанням ЕОМ, систем і комп'ютерних мереж для контролю над складними технологічними процесами, об'єктами та 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 траплялися випадки, коли в результаті незаконного втручання в роботу автоматизованих систем управління порушувався виробничий процес, створювалася загроза життю багатьох осіб.

[1] Див.: *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] *Former* Computer Network Administrator Guilty of Unleashing $10 Million Programming «Timebomb» (May 9, 2000).– Режим доступу: http://www.usdoj.gov/criminal/cybercrime/njtime.html

Поширення комп'ютерних технологій у Збройних силах дозволяє дійти висновку, що одним із можливих наслідків незаконного втручання може бути порушення обороноздатності держави. Наприклад, унаслідок 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 р. американський хакер Ерік Барнс у дні, коли НАТО бомбило Югославію, перекрутив інформацію, що знаходилася на офіційному сайті Білла 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].

На початку 80-х років шляхом перекручення інформації в комп'ютері, що керує роботою конвеєра Волзького автомобільного заводу, була на деякий час зупинена його робота[2]. Додатковим об'єктом у цьому випадку були суспільні відносини управління виробничими процесами. 1992 р. було вчинено умисне порушення роботи автоматизованої системи управління Ігналінської АЕС[3]. Тут додатковими об'єктами виступали відносини управління технологічними процесами та відносини забезпечення безпеки життя і здоров'я працівників. Досить цікавими, у контексті дослідження істотної шкоди, є приклади великих хакерських атак, що наводить О. Г. Шаваєв[4]. Так, у березні 1996 р. аргентинський хакер проник до таємних комп'ютерних мереж NASA, NORAD, міністерства оборони США, оборонних комп'ютерних мереж Великобританії, Тайваню, Мексики та ПАР; у липні 1997 р. було заблоковано один із каналів зв'язку центру керування польотами

[1] Див.: *Кабанников А.* Личный хакер Клинтона отправляется в тюрьму // Комсомольская правда.– 1999.– 24 ноября.– С. 3.

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

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

[4] Див.: *Шаваев А. Г.* Система борьбы с экономической разведкой.– М.: Издательский дом правовое просвещение, 2000.– С. 57–58.

NASA з космічним човном «Атлантіс»; у листопаді 1998 р. було знищено інформацію, яка містилася в електронних поштових скриньках 5 тис. студентів і співробітників Стенфордського університету; у січні 1999 р. невідомі змінили траєкторію польоту одного з британських супутників-шпигунів; у травні 1999 р. хакери на добу повністю змінили відомості, що містилися на сайті президента США; у січні 2000 р. невідомі вивели з ладу половину комп'ютерів Агентства національної безпеки США.

Слід зауважити, що визначити вичерпний перелік можливих наслідків комп'ютерного злочину надзвичайно важко, оскільки в кожному випадку ці наслідки залежать насамперед від змісту знищуваної або перекручуваної комп'ютерної інформації, який може бути різним. Характер значної шкоди в кожному конкретному комп'ютерному злочині, як правило, залежить від тих суспільних відносин, які є додатковим об'єктом. Це можуть бути відносини в різних сферах діяльності людини, пов'язані з використанням ЕОМ, систем і комп'ютерних мереж. Зашкоджуючи інформаційним відносинам, злочинець завдає або загрожує завдати шкоди тим суспільним відносинам, для інтенсифікації яких застосовується комп'ютерна техніка.

Отже, характер і розмір шкоди як кваліфікуючої ознаки комп'ютерного злочину залежить від змісту комп'ютерної інформації, яка є предметом посягання та характеристики додаткового об'єкта. Значна шкода може виражатись як у матеріальній, так і в іншій нематеріальній шкоді.

Суб'єктивна сторона комп'ютерного злочину, який заподіяв істотну шкоду, характеризується змішаною формою вини. У таких злочинах психічне ставлення особи до діяння та першого, обов'язкового, наслідку (втрати, підробки, блокування інформації тощо) виражається в умислі (прямому або непрямому), а до другого (кваліфікованого) наслідку – істотної шкоди – може бути як умисним, так і необережним. При цьому зауважимо, що в деяких випадках, умисне заподіяння істотної шкоди в результаті комп'ютерного злочину може фактично становити інший склад злочину. Наприклад, цілком очевидно, що знищення певної надзвичайно важливої для обороноздатності країни комп'ютерної інформації з метою ослаблення держави не є несанкціонованим втручанням, яке спричинило істотну шкоду (ч. 2 ст. 361 КК), а є нічим іншим як диверсією (ст. 113 КК).

Запитання для самоконтролю та самоперевірки

1. Охарактеризуйте інформаційні відносини як об'єкт злочину: предмет, суб'єкти, зміст.
2. Яка специфіка інформації як предмета права?
3. Визначіть співвідношення категорій «носій інформації» та «інформація»?
4. Наведіть визначення та розмежування понять «електронно-обчислювальна машина», «автоматизована система», «комп'ютерна мережа» та «мережа електрозв'язку».
5. Наведіть та проаналізуйте основні підходи до визначення поняття «комп'ютерний злочин».
6. Назвіть специфіку об'єктивної та суб'єктивної сторони комп'ютерних злочинів, що заподіюють істотну шкоду.
7. Коли комп'ютерний злочин вважається вчиненим повторно?
8. Коли комп'ютерний злочин вважається вчиненим за попередньою змовою групою осіб?

Розділ 3. Несанкціоноване втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

3.1. Безпосередній об'єкт несанкціонованого втручання в роботу комп'ютерної техніки та мереж електрозв'язку

Згідно із загальновизнаним положенням кримінального права в будь-якому складі злочину безпосередній об'єкт є частиною родового об'єкта, а тому відношення, яке є безпосереднім об'єктом, повинне охоплюватися сукупністю тих суспільних відносин, які становлять родовий об'єкт.

Як уже було визначено, родовим об'єктом злочинів, передбачених у розділі XVI КК, є сукупність інформаційних відносин у сфері використання ЕОМ, автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку. Ці відносини не є однорідними, тому завдання дослідження безпосереднього об'єкта несанкціонованого 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 несанкціонованого втручання є відносно новим, у літературі робилися спроби визначити його безпосередній об'єкт. Єдиної думки з цього питання немає. А. М. Ришелюк пропонує визначати його як нормальну роботу комп'ютерів і комп'ютерних мереж, а також як установлений порядок використання ЕОМ і комп'ютерних мереж[1]. Поділяючи наведену позицію,

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

А. В. Загіка визначає безпосередній об'єкт незаконного втручання як «відносини у сфері безпеки користування речовими та інтелектуальними засобами обчислювальної техніки»[1]. Деякі автори вважають, що таким об'єктом є «встановлений порядок обробки інформації в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах та передавання її каналами зв'язку»[2]. Здається, що такі визначення не відповідають специфіці несанкціонованого втручання і містять недолік, на який зверталась увага при розгляді родового об'єкта комп'ютерних злочинів: суспільні відносини, яким завдається шкода при скоєнні цього злочину, складаються не з приводу комп'ютерної техніки або безпеки її використання, а з приводу інформації, що опрацьовується ЕОМ, системами, комп'ютерними мережами або мережами електрозв'язку.

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 ґрунтувалася на тому, що в Законі України «Про інформацію» при характеристиці інформаційних відносин називалася така категорія, як «право власності на інформацію» (ст. 38)[3]. 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 розумітись і така категорія, як «власність на інформацію». Один із аргументів на підтвердження цієї думки може полягати в тому, що ефективність цивільно-правових інститутів багато в чому забезпечується наявністю санкцій за їх порушення. У ряді випадків, залежно від соціальної значущості цивільно-правового відношення, його охорона забезпечується нормами закону про кримінальну відповідальність. Так, наприклад, забезпечується ефективність цивільно-правового інституту власності на річ. Отже, якщо в кримінальному праві

[1] Див.: *Уголовный* кодекс Украины. Комментарий / Под ред. Ю. А. Кармазина и Е. Л. Стрельцова.– Х.: ООО «Одиссей», 2001.– С. 747.

[2] *Бутузов В. М., Остапець С. Л., Шеломенцев В. П.* Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: Науково-практичний коментар.– К.: Друкарня МВС України, 2005.– С. 14.

[3] Див.: *Закон* України «Про інформацію» від 02.11.1992 р. // Закони України.– К., 1996.– Т. 4.– С. 72–88.

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 про 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 матеріальними, речовими об'єктами, із речами»[1]. Подібної точки зору дотримується і Л. К. Терещенко, який доходить висновку, що класична «тріада» правомочностей власника, який має абсолютне право на річ, не може застосовуватися до інформації. До неї не можна застосовувати правомочність «володіння», оскільки не реально 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 вважає, що комп'ютерну інформацію[3] можна визнати предметом матеріального світу[4] і наводить такі аргументи. По-перше, відмічаючи, що згідно із законодавством до інформації можна застосовувати повноваження власника і що неможливо застосовувати зазначені повноваження

[1] Див.: *Гаврилов О. А.* Информатизация правовой системы России. Теоретические и практические проблемы.– М., 1998.– С. 61.

[2] Див.: *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: *Северин В. А.* Правовое регулирование информационных отношений // Вестник МГУ.– Серия 11. Право.– 2000.– № 5.– С. 24).

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

[4] Див.: *Кузнєцов В.* Комп'ютерна інформація як предмет крадіжки // Право України.– 1999.– № 7.– С. 86.

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.

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, на його думку, 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 не пов'язане з правом на матеріальний носій[1].

Аналіз різних точок зору дає можливість зробити ряд висновків, які мають велике 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 у разі застосування законодавцем до інформації таких понять, як «володіння», «користування» і «розпоряджання», 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 певну данину деяким стандартам і традиціям». За автором визнаються особливі авторські права, які забезпечують його інтерес як творця, але не як особи, котра володіє річчю[2]. Ще на початку XX ст. Т. Ф. Шершеневич

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

[2] Див.: *Суханов Е. А.* Курс лекций по гражданскому праву.– М., 1987.– С. 153.

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»[1]. Така ж ситуація спостерігається зараз і в правовому регулюванні інформаційних відносин. Застосування до інформації термінів «володіння», «користування» і «розпоряджання» зовсім не означає, що інформація прирівнюється до речі й інформаційні відносини регулюються правом власності на річ.

Необхідно також зауважити, 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»[2]. А. Б. Венгеров, досліджуючи правові аспекти інформатики, виділяв таку властивість інформації, як її самостійність відносно свого носія[3]. Крім того, коли інформація ототожнюється з носієм, то й право власності на інформацію ототожнюється з володінням, користуванням і розпоряджанням не інформацією, а її носієм, тобто з правом власності на річ. Можливість застосування для регулювання суспільних відносин з приводу комп'ютерної інформації права власності на річ у свою чергу досить справедливо піддано критиці в літературі.

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 прирівнювати до передавання речей[4].

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

[1] Див.: *Шершеневич Т. Ф.* Учебник русского гражданского права (по изданию 1907 г.).– М.: Фирма «Спартак», 1995.– С. 254–255.

[2] Див.: *Винер Н.* Кибернетика.– М., 1983.– С. 208.

[3] Наведено за: *Батурин Ю. М.* Проблемы компьютерного права.– М.: Юридическая литература, 1991.– С. 14.

[4] Див.: *Венгеров А. Б.* Категория «информация» в понятийном аппарате юридической науки // Советское государство и право.– 1977.– № 10.– С. 70–71.

– ці злочини посягають на різні предмети[1];

– інформація не має властивостей предмета злочинів проти власності, зокрема фізичної властивості[2].

Неодноразово в літературі підкреслювалося, що й норми про розкрадання майна не можна застосовувати для кваліфікації випадків копіювання комп'ютерної інформації[3].

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 зазначено, 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)[4]. Цю особливість 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[5].

Отже, правове регулювання суспільних відносин з приводу інформації за допомогою *інституту права власності на річ* не

[1] Див.: *Уголовное* право. Особенная часть: Учебник / Под ред. проф. А. И. Рарога.– М.: Институт международного права и экономики. Изд-во «Триада, Лтд», 1997.– С. 231.

[2] Див.: *Комментарий* к Уголовному кодексу Российской Федерации / Отв. ред. докт. юрид. наук, проф. А. В. Наумов.– М.: Юристъ, 1996.– С. 662–663.

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

[4] Див.: *Stein* Schjolberg, Chief Judge Moss byrett, Norway «The Legal Framework – Unauthorized Access to Computer Systems. Penal Legislation in 37 Countries».– Режим доступу: http://www.mossbyrett.of.no/legal.html

[5] *International* review of criminal policy – United Nations Manual on the prevention and control of computer-related crime, paragraph 86–87.– Режим доступу: http://www.ifs.univie.ac.at/~pr2qq/rew4344.html

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 й 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 річ 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 правового регулювання й охорони суспільних відносин у цій сфері. Це пояснюється тим, що інформація й 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.

Ураховуючи 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 певну обережність у поширенні на неї правовідносин власності. Однак, незважаючи на безсумнівну специфіку, інформація поза відносинами власності 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.*

Інформація як предмет права власності є за своїм змістом *сприймані та використовувані людиною відомості про об'єктивний світ і процеси, що відбуваються в ньому.*

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

Як уже зазначалося раніше, інформація не існує без носія і «сама по собі» в систему суспільних відносин включена бути не може. Необхідною передумовою власності на інформацію є *володіння її носієм*. Зважаючи на це, доцільно володіння як елемент права власності на інформацію визначати як *наявність в особи права та можливості володіння носієм інформації.*

Право користування є наявністю в особи права та можливості задовольняти за допомогою інформації свої потреби. Здійснюючи право 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 із приводу інформації, як ми зазначали вище, не забезпечує їх адекватного правового відображення. Задоволення інформаційної потреби здійснюється шляхом використання інформаційних властивостей носія. Використання у процесі створення механізму правового регулювання відносин із приводу інформації описаної специфіки інформації як предмета правового регулювання дає змогу усунути ототожнення інформації з її носієм. Отже, право користування інформацією можна визначити таким чином: *наявність в 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 є формою реалізації цих відносин і відображає соціальний інтерес розповсюдження інформації. Отже, право розпоряджання інформацією слід визна-

чати таким чином: *наявність в 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 – належать 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 (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 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, відбивається у *праві володіння*.

Отже, безпосереднім об'єктом несанкціонованого втручання 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 досить повно відображає 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.

Необхідно зауважити, що зміни в редакції ст. 361 КК (закони України «Про внесення змін до Кримінального кодексу України щодо відповідальності за незаконне втручання в роботу мереж електрозв'язку» від 5 червня 2003 р. та «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» від 23 грудня 2004 р.) зумовили появу нових характеристик безпосереднього об'єкта несанкціонованого втручання. Нова редакція аналізованої статті дає підстави стверджувати, що, крім права власності на комп'ютерну інформацію, нею охороняються й *суспільні відносини надання та отримання послуг електричного зв'язку*. До цих суспільних відносин можна застосувати термін «альтернативний безпосередній об'єкт злочину». Цілком зрозуміло, що введення його потребує серйозної аргументації та окремого дослідження, однак, на нашу думку, специфіка чинної редакції ст. 361 КК України полягає в тому, що вона забезпечує охорону від злочинних посягань двох різних видів суспільних відносин: власності на комп'ютерну інформацію та надання послуг електричного зв'язку.

Як ми вже зазначали, досить поширеним є визначення об'єкта аналізованого злочину як безпеки інформації та систем опрацювання інформації з використанням ЕОМ або порядку опрацювання інформації. Якщо визнати цю позицію правильною, то можна було б уникнути питання про альтернативний безпосередній об'єкт незаконного втручання і, з урахуванням чинної редакції ст. 361 КК, визначити безпосередній об'єкт незаконного втручання таким чином: суспільні відносини, що забезпечують безпеку (або порядок) використання ЕОМ, систем, комп'ютерних мереж і мереж електрозв'язку.

Однак наведене визначення, як видається, не відповідало б сутності несанкціонованого втручання як посягання не з приводу

автоматизованих систем або мереж електрозв'язку, а з приводу інформації, яка опрацьовується комп'ютерною технікою, або послуг електрозв'язку, для надання яких використовується відповідна мережа. Крім того, логічним наслідком визнання безпосереднім об'єктом досліджуваного злочину відносин, що забезпечують безпеку використання комп'ютерної техніки або мереж електрозв'язку, буде відсутність чітких критеріїв визначення суспільної небезпечності конкретного посягання. Розглянемо два приклади:

1) особа незаконно втручається в роботу ЕОМ і знищує інформацію про новітні наукові розробки;

2) особа незаконно втручається в роботу ЕОМ і знищує інформацію неістотного змісту, яка зовсім не впливає на діяльність її власника.

Цілком зрозуміло, що ступінь суспільної небезпечності незаконного втручання в другому прикладі, на відміну від першого, недостатній для визнання такого діяння злочином. Однак, якщо визначати об'єкт несанкціонованого втручання як безпеку (або порядок) використання засобів комп'ютерної техніки, ці два приклади слід розглядати як такі, що мають однаковий ступінь суспільної небезпечності. Адже і в першому, і в другому було заподіяно приблизно однакову шкоду безпеці (або порядку) використання ЕОМ. Ще раз зауважимо: *суспільні відносини, яким завдається шкода при скоєнні несанкціонованого втручання, складаються не з приводу комп'ютерної техніки, безпеки або порядку її використання чи безпеки використання мереж електрозв'язку, а з приводу інформації, що опрацьовується ЕОМ, системами, комп'ютерними мережами, та інформації, яка отримується або передається з використанням мереж електрозв'язку.*

Отже, ст. 361 *охороняє, крім відносин власності на комп'ютерну інформацію, суспільні відносини надання послуг електрозв'язку.* Відповідно до змісту Закону України «Про телекомунікації» від 18 листопада 2003 р. всі мережі електрозв'язку поділяються на мережі загального користування (мережі, доступ до яких відкрито для всіх споживачів телекомунікаційних послуг) та мережі спеціального користування. Зміст цих відносин полягає в тому, що оператори та провайдери телекомунікацій забезпечують їх споживачам можливість передавання та приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень

будь-якого роду за допомогою радіо, проводових, оптичних або інших електромагнітних систем. Слід ще раз наголосити, що різниця суспільних відносин власності на інформацію, пов'язаних із використанням комп'ютерних мереж, і суспільних відносин надання й отримання послуг електрозв'язку полягає в тому, що згідно зі змістом ст. 361 КК та Закону України «Про телекомунікації» до мереж електрозв'язку відносяться всі телекомунікаційні мережі, крім комп'ютерних.

3.2. Предмет несанкціонованого втручання

Предметом злочину, передбаченого ст. 361 КК України, судячи з диспозиції, є *інформація,* але аналіз об'єкта і форм об'єктивної сторони несанкціонованого втручання дає підстави стверджувати, що до предметів даного злочину відносяться комп'ютерна інформація та інформація, що передається каналами зв'язку.

Комп'ютерна інформація. Об'єкт і предмет будь-якого злочину є взаємозалежними, взаємозумовленими. Тому, аналізуючи ознаки предмета несанкціонованого втручання, необхідно виходити з викладеної вище характеристики змісту безпосереднього об'єкта як *відносин власності на інформацію.* Загальновизнаною в кримінальному праві є точка зору, що предмет злочину характеризується сукупністю трьох ознак: фізичної, економічної та юридичної. Тому, визначаючи інформацію предметом злочину, 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. 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, котрий зазвичай розуміється як предмет, річ, властивості якої використовуються для передання, зберігання та обробки інформації. Носіями комп'ютерної інформації є дискети, оптичні та жорсткі диски і т. ін. Визначаючи носій комп'ютерної інформації, необхідно враховувати, що однією з найважливіших характеристик сучасного етапу комп'ютеризації є розвиток електронних засобів зв'язку. Тому

деякі дослідники[1] ставлять питання про статус інформації, що передається каналами зв'язку. Передається вона за допомогою сигналів, які теж є матеріальними носіями передання 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 випадки впливу не тільки на пристрої комп'ютера, але й на сигнали, які 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 якого використовуються для зберігання, передавання й опрацювання інформації, що розпізнається ЕОМ.*

Інформація як предмет злочину має *економічну ознаку,* ціну, яка врешті-решт визначається її змістом і заінтересованістю споживача в її одержанні. Економісти відмічають, що як товар інформація має цілу низку специфічних властивостей: «незнищуваність у процесі споживання; можливість багатократного споживання багатьма користувачами; у процесі передавання споживачеві 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 агентів; виробникові інформації заздалегідь споживач невідомий; неможлива однозначна вартісна оцінка виробленого обсягу інформації; особливий механізм її старіння – вона не зношується, а втрачає актуальність»[3]. 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. Зважаючи на це, до економічної ознаки комп'ютерної інформації слід віднести не тільки наявність ціни, але й наявність *корисних властивостей*, які дають можливість задовольняти інформаційну потребу. Ці властивості можна описати так:

– *цілісність* – захищеність від несанкціонованих змін;

– *доступність* – захищеність від несанкціонованого змісту інформаційних ресурсів;

– *конфіденційність* – захищеність від несанкціонованого одержання комп'ютерної інформації[1].

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

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

Отже, комп'ютерну інформацію як предмет злочину, виходячи з викладеного, 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.***

Інформація, що передається каналами зв'язку. Співвідношення категорій «інформація, що передається мережами електрозв'язку» та «комп'ютерна інформація», яка теж відноситься до предметів незаконного втручання, можна визначити таким чином: якщо комп'ютерна інформація – це відомості, подані у формі, яка дозволяє опрацьовувати їх за допомогою ЕОМ, то інформацією, що передається мережами електрозв'язку, є ***відомості, подані у формі, що дозволяє їх приймати або передавати засобами електрозв'язку.*** Інформація в цих мережах передається за допомогою сигналів, які є матеріальними носіями передавання інформації. Слід

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

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

[3] Див.: *Новиков О. А., Мясникова Л. А.* Логистика и коммерция информационного общества // Проблемы развития внешнеэкономических связей и привлечения иностранных инвестиций: региональный аспект: Сб. науч. трудов.– Донецк, 1999.– С. 118.

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

зауважити, що електричні сигнали в мережах електрозв'язку можуть бути носіями комп'ютерної інформації. Наприклад, у комп'ютерних мережах телефонні лінії використовуються для зв'язку між ЕОМ, що знаходяться в мережі. У такому разі інформація, що передається мережею електрозв'язку, є комп'ютерною, а її знищення чи перекручення треба розглядати як наслідок несанкціонованого втручання в роботу комп'ютерної мережі.

3.3. Об'єктивна сторона несанкціонованого втручання в роботу електронно-обчислювальних машин, систем, комп'ютерних мереж і мереж електрозв'язку

Диспозиція ст. 361 КК України дає змогу зробити висновок про те, що об'єктивна сторона несанкціонованого втручання характеризується такою структурою: *діяння* – несанкціоноване втручання в роботу ЕОМ, систем, комп'ютерних мереж і мереж електрозв'язку; *суспільно небезпечні наслідки* – витік, втрата, підробка, блокування інформації, спотворення процесу обробки інформації, порушення встановленого порядку маршрутизації інформації (перелічені наслідки є альтернативними, тобто для наявності складу злочину достатньо настання хоча б одного з наслідків); *причиновий зв'язок між діянням та наслідками*.

Стосовно визначення несанкціонованого втручання серед науковців немає єдиної точки зору. Так, деякі автори вважають що воно може проявлятися в несанкціонованому доступі, що розуміється як доступ до інформації, пов'язаний з подоланням програмних, технічних чи організаційних заходів захисту, або в несанкціонованому впливі на інформацію, що здійснюється з порушенням методів і процедур автоматизованого опрацювання інформації[1]. Стаття 361 КК не містить вказівки на те, що несанкціоноване втручання обов'язково має супроводжуватися подоланням засобів

[1] Див.: *Бутузов В. М., Остапець С. Л., Шеломенцев В. П.* Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: Науково-практичний коментар.– К.: Друкарня МВС України, 2005.– С. 15–17.

захисту інформації. Отже, таке визначення є не зовсім вдалим. А. А. Музика та Д. С. Азаров визначають несанкціоноване втручання як вплив на інформаційні процеси за умови, що він є несанкціонованим. При цьому зазначається, що фізичний вплив безпосередньо на ЕОМ, автоматизовані системи, комп'ютерні мережі та мережі електрозв'язку чи відповідні носії інформації не охоплюється складом злочину, передбаченого ст. 361 КК України. На думку названих авторів, такі діяння, вчинені з метою заволодіння, знищення, пошкодження, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку маршрутизації інформації, за наявності підстав можуть кваліфікуватися за ст. 360 КК або як відповідний злочин проти власності[1]. Коментуючи цю позицію, зазначимо, що вона є більш вдалою, але має схожий недолік: диспозиція ст. 361 не обмежує спосіб вчинення діяння, вона не містить указівки на те, що діяння не може бути вчинене шляхом безпосереднього фізичного впливу на засоби комп'ютерної техніки або телекомунікації.

Аксіомою є таке положення: діяння, що належить до об'єктивного боку складу злочину, є суспільно небезпечним, тобто заподіює істотну шкоду суспільним відносинам, охоронюваним кримінальним законом, або створює реальну загрозу її заподіяння[2]. Тобто, зміст діяння визначається об'єктом злочину, діянням є дія або бездіяльність, яка заподіює або може заподіяти шкоду об'єкту. Оскільки, як було зазначено раніше, безпосередній об'єкт досліджуваного злочину характеризується певною подвійністю, можна виокремити такі види несанкціонованого втручання, які розрізняються за змістом:

– несанкціоноване втручання в роботу ЕОМ, автоматизованих систем і комп'ютерних мереж;

– несанкціоноване втручання в роботу мереж електрозв'язку.

Виділення видів несанкціонованого втручання на підставі специфіки об'єкта дає можливість сформулювати ще одне положення: зміст ознак несанкціонованого втручання в роботу комп'ютерної техніки визначається тим, що воно заподіює шкоду відносинам

[1] Див.: *Законодавство* про кримінальну відповідальність за «комп'ютерні» злочини: Науково-практичний коментар і шляхи вдосконалення / А. А. Музика, Д. С. Азаров.– К.: Вид. Паливода А. В., 2005.– С. 26–29.

[2] Див.: *Кримінальне* право України. Загальна частина: Підручник / М. І. Бажанов, Ю. В. Баулін, В. І. Борисов та ін.; За ред. проф. М. І. Бажанова, В. В. Сташиса, В. Я. Тація.– 2-е вид., переробл. і доп.– К.: Юрінком Інтер, 2004.– С. 119–120.

власності на комп'ютерну інформацію, а несанкціонованого втручання в роботу мереж електрозв'язку – тим, що воно заподіює шкоду відносинам надання й отримання послуг електрозв'язку.

Втручання в роботу ЕОМ, систем або комп'ютерних мереж слід розуміти як зміну режиму роботи ЕОМ, системи, комп'ютерної мережі. Конкретизуємо зміст ознак цього діяння, установивши його фізичну, соціальну та юридичну ознаки. *Фізична* ознака втручання виявляється в тому, що воно полягає у впливі на матеріальний носій комп'ютерної інформації або засоби її автоматизованого опрацювання. Суспільна небезпечність (*соціальна* ознака) несанкціонованого втручання визначається тим, що діяння ставить під загрозу функціонування ЕОМ, систем і комп'ютерних мереж у сфері зберігання, опрацювання, зміни, доповнення, передавання й одержання інформації, тобто заподіює шкоду суспільним відносинам права власності на комп'ютерну інформацію. *Протиправність* як обов'язкова ознака аналізованого діяння характеризується в законі за допомогою терміна «несанкціоноване». Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31 травня 2005 р. під несанкціонованими діями щодо інформації в системі розуміються дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

Викладене дає можливість навести таке визначення несанкціонованого втручання в роботу ЕОМ, систем або комп'ютерних мереж: *зміна режиму роботи ЕОМ, системи або комп'ютерної мережі, вчинена шляхом впливу на носій комп'ютерної інформації або засоби її автоматизованого опрацювання, з порушенням встановленого відповідно до законодавства порядку доступу до інформації, що заподіює шкоду суспільним відносинам власності на комп'ютерну інформацію.*

Значний інтерес при аналізі несанкціонованого втручання в роботу ЕОМ, систем або комп'ютерних мереж становить питання про способи вчинення цього злочину. 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 несанкціонованого втручання видається необхідною.

Різні способи несанкціонованого 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:

1) способи, що ґрунтуються на використанні засобів фізичного впливу;

2) способи, що ґрунтуються на використанні програмного забезпечення;

3) змішані способи.

Способи першої групи характеризуються тим, що комп'ютерні технології, як будь-який інший прилад або пристрій, не є абсолютно надійними. Під час роботи з ними досить 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, унаслідок 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 як «вплив на технічні засоби, який приводить до здійснення загрози для інформації»[1]. Вчинення незаконного втручання таким способом, як правило, пов'язане з використанням спеціальних приладів. Наприклад, існують заряди електромагнітної дії, після вибуху яких на досить великому радіусі припиняють роботу комп'ютери та засоби зв'язку[2]. Така група способів пов'язана з *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 злочини 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

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

[2] Див.: *Кабанников А.* Электронная «Хиросима» уже затаилась в Москве // Комсомольская правда.– 1998.– 16 декабря.– С. 5.

майна (комп'ютерної техніки), то має місце злочин проти власності; у випадку ж, коли дії злочинця спрямовані на заподіяння шкоди відносинам власності на комп'ютерну інформацію, то мова може йти про ідеальну сукупність несанкціонованого втручання в роботу ЕОМ, системи або комп'ютерної мережі та умисного пошкодження майна.

Друга група способів скоєння досліджуваного злочину ґрунтується 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 стосовно комп'ютерної інформації. Специфічною рисою цих способів є те, що комп'ютер продовжує функціонувати, але інформація, яка опрацьовується в ньому, знищується, перекручується, копіюється тощо. Наприклад, особа проникла до приміщення, де розташована електронно-обчислювальна машина, і з використанням стандартної програми Windows «Провідник» незаконно знищила певну інформацію.

Третя група – змішані способи – ґрунтується 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.

До наслідків несанкціонованого втручання в роботу ЕОМ, систем або комп'ютерних мереж відносяться: 1) витік; 2) втрата; 3) підробка; 4) блокування комп'ютерної інформації; 5) спотворення процесу обробки комп'ютерної інформації; 6) порушення встановленого порядку маршрутизації комп'ютерної інформації.

Безперечним є те, що якісні характеристики суспільно небезпечних наслідків залежать від змісту об'єкта посягання. На думку Н. Ф. Кузнєцової, злочинний наслідок – це сполучна ланка між об'єктом і злочинним діянням[2]. А. А. Пінаєв наголошує, що наслідки визначаються об'єктом злочину[1]. Отже, цілком обґрунтованим буде таке положення: перелічені суспільно небезпечні наслідки несанкціонованого втручання в роботу ЕОМ, систем або комп'ютерних мереж є різними формами порушення права власності на комп'ютерну інформацію.

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

[2] Див.: *Кузнецова Н. Ф.* Значение преступных последствий для уголовной ответственности.– М.: Государственное изд-во юридической лит-ры, 1958.– С. 10.

Так, *витік* інформації, відповідно до ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31 травня 2005 р.,– це результат дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї. Витік є порушенням такого повноваження власника комп'ютерної інформації, як право розпорядження.

Термін *«втрата комп'ютерної інформації»*, як видається, є тотожним терміна «знищення комп'ютерної інформації». Зазначимо, що в літературі немає єдиної думки стосовно змісту цього поняття. Деякі вчені вважають, що під знищенням інформації слід розуміти стирання її в пам'яті ЕОМ[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». Зміст цей 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 непридатний для використання за призначенням стан[4] або припинення існування комп'ютерної інформації, приведення її в такий стан, коли її не можна відновити або використати

[1] Див.: *Пинаев А. А.* Уголовно-правовая борьба с хищениями.– Х.: Вища школа, 1975.– С. 58.

[2] Див.: *Комментарий* к Уголовному кодексу Российской Федерации.– 2-е изд., изм. и доп. / Под общ. ред. Ю. И. Скуратова и В. М. Лебедева.– М.: Издательская группа Норма-Инфра-М, 1998.– С. 415.

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

[4] Див.: *Уголовный* кодекс Российской Федерации. Постатейный комментарий.– С. 583.

за призначенням[1]. Однак і ці визначення є неповними, оскільки не відбивають такої ознаки наслідку, як протиправність, не дають змоги з'ясувати ті правові відносини, яким знищення інформації може завдати шкоди. Крім того, неповнота наведених визначень поняття знищення комп'ютерної інформації виявляється в тому, що вони не відбивають специфіки безпосереднього об'єкта цього злочину.

Думається, що повніше суть досліджуваного наслідку – порушення повноваження володіння власника комп'ютерної інформації – буде розкрито в такому визначенні: *втрата комп'ютерної інформації – це такий вплив на носій комп'ютерної інформації, унаслідок якого вона перестає існувати у формі, яка дозволяє опрацьовувати її за допомогою комп'ютерної техніки.*

Слід зазначити, що комп'ютерна інформація, у 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 носієві, яке відповідає такому файлу, вважається вільним, тому інформація фактично втрачається лише після того, як на це місце буде записано нову інформацію. Тобто, у власника певний час є можливість відновити знищену інформацію. Правильним видається вирішення цього питання, запропоноване А. Г. Волеводзом, 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[2].

Підробка комп'ютерної інформації, як видається, є порушенням такого повноваження власника як користування, адже через підробку власник повністю або частково втрачає можливість реалізовувати свою інформаційну потребу. Виходячи з цього, можна визначити підробку комп'ютерної інформації таким чином: *зміна без відома власника змісту відомостей, відображених на носії, що робить інформацію цілком або частково непридатною для задоволення інформаційної потреби особою, яка має право власності на таку інформацію.*

[1] Див.: *Комментарий* к Уголовному кодексу Российской Федерации / Отв. ред. В. И. Радченко.– М.: Вердикт, 1996.– С. 646.

[2] Див.: *Волеводз А. Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества.– М.: ООО Изд-во «Юрлитинформ», 2002.– С. 67–68.

Блокування комп'ютерної інформації також є специфічною формою порушення повноваження користування інформацією. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31 травня 2005 р. містить термін «блокування інформації в системі», який визначається таким чином: дії, унаслідок яких унеможливлюється доступ до інформації в системі. Отже, блокування є ситуацією, коли комп'ютерна інформація не знищена, не підроблена, але можливість використовувати її відсутня. Можна сформулювати таке визначення: *блокування комп'ютерної інформації – відсутність у власника можливості використовувати інформацію для задоволення інформаційної потреби за умови, що її не втрачено та не підроблено.*

Прикладом несанкціонованого втручання в роботу комп'ютерної мережі, що призвело до блокування інформації, можуть слугувати так звані розподілені атаки відмови від обслуговування (DDoS-атаки, Distributed Denial of Service attacks), які полягають у направленні дуже великої кількості запитів на один або кілька серверів, що викликає їх перевантаження та призводить до того, що інформаційний ресурс, доступ до якого забезпечується сервером, стає недоступним.

Спотворення процесу обробки комп'ютерної інформації. Обробка інформації в автоматизованій системі відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31 травня 2005 р. є виконанням однієї або кількох операцій, зокрема збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів. З урахуванням цього спотворення процесу обробки комп'ютерної інформації можна визначити як *отримання в результаті операцій з комп'ютерною інформацією, які здійснювалися за допомогою технічних чи програмних засобів, результатів, що не відповідають характеристикам технічних засобів або алгоритму комп'ютерної програми.*

Порушення встановленого порядку маршрутизації комп'ютерної інформації матиме місце, коли комп'ютерна інформація, що передається за допомогою комп'ютерної мережі конкретному абонентові (абонентам), ним не отримується або доступ до певних мережевих ресурсів здійснюється з порушенням встановленого порядку.

Для прикладу несанкціонованого втручання в роботу комп'ютерної мережі розглянемо вирок Корольовського районного суду м. Житомира по справі № 1-162/2009 від 5 березня 2009 р.[1] щодо обвинувачення В. Крім кваліфікованої крадіжки, передбаченої ч. 3 ст. 185 КК, обставини вчинення якої ми аналізувати не будемо, він обвинувачувався у вчиненні злочину, передбаченого ч. 1 ст. 361 КК України. Так, 05.11.2008 р. близько 13 год, знаходячись за місцем свого проживання, використовуючи власний персональний комп'ютер та викрадений комутатор фірми «Zyxel» модель «ES-2108», до мережевих налаштувань якого він довільно ввів IP-адресу XXX.XX.XX.XXX, несанкціоновано втрутився в роботу комп'ютерної мережі DKS через незаконне підключення до неї та використання її інформаційних ресурсів у власних інтересах, що призвело до блокування інформації та порушення встановленого порядку її маршрутизації, оскільки законним абонентам цієї комп'ютерної мережі було блоковано вихід до цієї мережі, доступ до її ресурсів і використання послуг оператора.

Суд правильно кваліфікував дії В., як *несанкціоноване втручанням в роботу комп'ютерної мережі DKS*, що призвело до *блокування* інформації (яке полягає в тому, що абонентам, робота в мережі яких проходила через сервер з IP-адресою XXX.XX.XX.XXX, було блоковано вихід у комп'ютерну мережу DKS та доступ до ресурсів цієї мережі і використання послуг оператора) і *порушення встановленого порядку її маршрутизації* (яке полягає в тому, що особа, яка не має законного права користуватися ресурсами комп'ютерної мережі DKS, отримала до неї доступ, не передбачений власником мережі).

Несанкціоноване втручання в роботу мережі електрозв'язку є зміною режиму її роботи. Оскільки, як було зазначено, до складу мережі електрозв'язку входять технічні засоби та споруди зв'язку, *фізичну властивість* несанкціонованого втручання в роботу мережі електрозв'язку можна визначити як *зміну режиму роботи мережі, що вчинена шляхом впливу на засоби або споруди зв'язку*. Суспільна небезпечність такого діяння, його *соціальна* ознака полягають у тому, що воно ставить під загрозу суспільні відносини щодо надання й отримання послуг електрозв'язку,

[1] Вирок Корольовського районного суду м. Житомира по справі № 1-162/2009 від 5 березня 2009 р. // Єдиний державний реєстр судових рішень.– Режим доступу: http://www.reyestr.court.gov.ua/

унаслідок цього діяння абоненти мережі отримують неякісні послуги зв'язку або не отримують їх зовсім. *Протиправність* як обов'язкова ознака несанкціонованого втручання в роботу мереж електрозв'язку полягає в тому, що це діяння є порушенням установленого нормативно-правовими актами режиму користування мережами електрозв'язку. Отже, можна запропонувати таке визначення: *несанкціоноване втручання в роботу мережі електрозв'язку – порушення встановленого режиму роботи мережі, вчинене шляхом впливу на засоби або споруди зв'язку, що ставить під загрозу суспільні відносини щодо надання й отримання послуг електрозв'язку.*

До наслідків несанкціонованого втручання в роботу мереж електрозв'язку відносяться: 1) витік; 2) втрата; 3) підробка; 4) блокування інформації, що передається каналами зв'язку; 5) порушення встановленого порядку маршрутизації інформації, що передається каналами зв'язку. Специфіка об'єкта і предмета цього посягання визначає й особливості змісту його суспільно небезпечних наслідків.

Отже, *витік* інформації, що передається мережею електрозв'язку, можна визначити за аналогією з витоком комп'ютерної інформації таким чином: результат несанкціонованого втручання в роботу мережі електрозв'язку, унаслідок якого інформація, що передається мережею, стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.

Втрата інформації, що передається мережами електрозв'язку,– це порушення електрозв'язку у виді неотримання абонентом мережі інформації, якому вона надсилається.

Підробкою інформації буде такий вплив на носій інформації, що передається мережею електрозв'язку, у результаті якого абонент отримує відомості, які не збігаються з тими, що було йому надіслано.

Блокування інформації, що передається каналами зв'язку, є результатом несанкціонованого втручання в роботу мережі електрозв'язку у виді неможливості або значного ускладнення протягом певного часу отримувати чи надсилати інформацію за допомогою цієї мережі.

Порушення порядку маршрутизації інформації в мережі електрозв'язку як правило матиме місце, коли інформація, що передається за допомогою мережі конкретному абонентові (абонентам), ним не отримується, а також у випадках отримання інформації, що пере-

дається в мережі, на кінцеве обладнання, яке не є складовою даної мережі. Типовими прикладами несанкціонованого втручання в роботу мереж електрозв'язку з настанням таких наслідків є незаконне підключення телефонних апаратів до мереж телефонного зв'язку, а також незаконне підключення телевізійних приймачів до мереж кабельного телебачення[1]. Однак зазначимо, що існують і більш складні види порушення порядку маршрутизації, які пов'язані, зокрема, з маршрутизацією вхідного міжнародного трафіку на телефонні мережі загального користування. У судовій практиці такий вид досліджуваних наслідків траплявся в контексті правової оцінки осіб, які займалися незаконною діяльністю щодо надання послуг IP-телефонії[2].

Під *спотворенням процесу обробки* інформації, що передається каналами електрозв'язку, необхідно розуміти отримання в результаті роботи технічного засобу зв'язку результатів, які не відповідають його характеристиці. Необхідно зазначити, що підробка та спотворення процесу обробки інформації в мережі електрозв'язку можуть характеризуватися спільним суспільно небезпечним результатом (заподіянням об'єкту однакової шкоди), проте різним є механізм її заподіяння – підробка вчиняється шляхом впливу на носій інформації, а спотворення процесу оброблення – шляхом впливу на технічний засіб зв'язку.

Причиновий зв'язок як обов'язкова ознака об'єктивної сторони несанкціонованого втручання в роботу ЕОМ, систем, комп'ютерних мереж або мереж електрозв'язку полягає в тому, що діяння (несанкціоноване втручання) з необхідністю спричиняє настання наслідків: воно передує настанню зазначених суспільно небезпечних наслідків, містить у собі реальну можливість наслідків і в конкретному випадку є необхідною умовою, без якої б наслідки не настали.

Несанкціоноване втручання буде закінченим з моменту настання суспільно небезпечних наслідків.

Для прикладу несанкціонованого втручання в роботу мережі електрозв'язку розглянемо вирок Придніпровського районного суду м. Черкаси по справі № 1-223/07 від 12 червня 2007 р.[1] щодо обвинувачення Л. у вчиненні злочину, передбаченого ч. 2 ст. 361 КК України. Підсудний умисно, без дозволу власника телефону ХХХ-ХХХ К., яка згідно договору про надання послуг електрозв'язку від 09.10.1999 р., є абонентом ВАТ «Укртелеком», 2, 3, 4, 6, 17, 19, 23 листопада 2006 р., з метою незаконного отримання для себе телефонних послуг здійснив несанкціоноване втручання до робочої мережі електрозв'язку, що виразилося у підключенні до її телефонного номеру, та здійсненні телефонних розмов за послугою «Аудіотекст».

Враховуючи означене, а також те, що підсудний у подібний спосіб незаконно підключався ще до телефонних номерів трьох інших власників, суд правильно кваліфікував його дії як *несанкціоноване втручання в роботу мережі електрозв'язку*, яке спричинило *блокування* інформації абонента, що виразилося у неможливості користування абонентом телекомунікаційними послугами, та *порушення встановленого порядку маршрутизації,* внаслідок чого телекомунікаційна інформація ВАТ «Укртелеком» фактично не надходила до кінцевого обладнання дійсного абонента, хоча обладнання ВАТ «Укртелеком» фіксувало користування абонентом послугою, *вчинене повторно*.

---

[1] Див.: Вироки Новокаховського міського суду Херсонської області по справі № 1-266/08 від 13 червня 2008 р. та по справі № 1-344/08 від 19 серпня 2008 р.; вирок Замостянського районного суду м. Вінниці по справі № 1-249/08 від 27 березня 2008 р. // Єдиний державний реєстр судових рішень.– Режим доступу: http://www.reyestr.court.gov.ua/. Коментуючи дані вироки, зазначимо, що суди правильно кваліфікують випадки незаконного підключення до мереж кабельного телебачення як несанкціоноване втручання в роботу мереж електрозв'язку – злочин, передбачений ст. 361. При цьому до подібних наслідків обґрунтовано відносять: *виток* інформації, оскільки програми мовлення, що транслюються в мережі отримуються особою в якої не має на це прав; *порушення порядку маршрутизації*, оскільки внаслідок дій порушника змінюється встановлений режим роботи мережі (збільшується кількість кінцевого обладнання) та у разі фіксації зменшення якості сигналу внаслідок дій порушника; *блокування* інформації, що передається мережами електрозв'язку.

[2] Див.: Вирок Кіровського районного суду м. Кіровограда по справі № 1-43/09 від 22 січня 2009 р. // Єдиний державний реєстр судових рішень.– Режим доступу: http://www.reyestr.court.gov.ua/

[1] Вирок Придніпровського районного суду м. Черкаси по справі № 1-223/07 від 12 червня 2007 р. // Єдиний державний реєстр судових рішень.– Режим доступу: http://www.reyestr.court.gov.ua/

3.4. Суб'єктивні ознаки несанкціонованого втручання в роботу електронно-обчислювальних машин, систем, комп'ютерних мереж і мереж електрозв'язку

Суб'єкт несанкціонованого втручання загальний, ним є фізична, осудна особа, що досягла 16-річного віку.

Суб'єктивна сторона несанкціонованого втручання виражається в тому, що особа: а) усвідомлювала суспільну небезпечність втручання, тобто фактичні та соціальні ознаки діяння, його несанкціонованість; б) передбачала наслідки у виді витоку, втрати, підробки, блокування інформації, спотворенні процесу обробки інформації або порушенні порядку її маршрутизації; в) бажала або свідомо припускала настання цих наслідків. Тобто, суб'єктивна сторона аналізованого складу може виражатися у виді як прямого, так і непрямого умислу.

Усвідомлення фактичних ознак несанкціонованого втручання полягає в тому, що особа усвідомлює закономірності функціонування ЕОМ, автоматизованої системи, комп'ютерної мережі або мережі електрозв'язку, використання яких дає можливість здійснювати втручання в їх роботу. Причому зрозуміло, що вимога усвідомлення об'єктивних ознак несанкціонованого втручання як точного, всебічного знання про всі процеси, що відбуваються в ЕОМ під час втручання, буде неправильною. Це пов'язано з тим, що функціонування ЕОМ – це надзвичайно складний і багатоплановий процес. Тому особа, яка здійснює несанкціоноване 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 в 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 накопичувачеві 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 напруження електромагнітного поля комп'ютерна інформація буде знищена або перекручена. На сьогодні досягнення у сфері виробництва апаратних засобів і програмного забезпечення привели до ситуації, коли детальне знання про процеси, що відбуваються під час роботи ЕОМ, не є обов'язковим для виконання завдань опрацювання інформації із 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 несанкціонованого 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 й можуть призвести до певних наслідків.

Усвідомлення несанкціонованості в цьому складі злочину зумовлене насамперед розумінням об'єкта, котрим, 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 ЕОМ, автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку. Наявність в особи права на інформацію або наявність у неї 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).

Запитання для самоконтролю та самоперевірки

1. Проаналізуйте висловлені в науці пропозиції щодо визначення безпосереднього об'єкта несанкціонованого втручання.
2. Право власності на інформацію як об'єкт несанкціонованого втручання.
3. Охарактеризуйте ознаки комп'ютерної інформації як предмета злочину.

---

[1] Див.: *Трайнин А. Н.* Состав преступления по советскому уголовному праву.– М.: Государственное изд-во юридической лит-ры, 1951.– С. 218.

4. У чому специфіка такого предмета несанкціонованого втручання, як інформація, що передається мережами електрозв'язку?

5. Охарактеризуйте об'єктивну сторону несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем і комп'ютерних мереж.

6. Яка класифікація способів вчинення несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем і комп'ютерних мереж?

7. Визначіть зміст ознак об'єктивної сторони несанкціонованого втручання в роботу мереж електрозв'язку.

8. Назвіть специфічні риси суб'єктивної сторони несанкціонованого втручання.

Розділ 4. Кримінальна відповідальність за незаконні дії зі шкідливими програмними або технічними засобами

4.1. Об'єкт і предмет створення, розповсюдження або збуту шкідливих програмних і технічних засобів

Безпосередній об'єкт злочину, передбачений ст. 361-1 КК, становлять суспільні відносини власності на комп'ютерну інформацію та відносини надання й отримання послуг електрозв'язку.

До *предметів* злочину відносяться:

– шкідливі програмні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

– шкідливі технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

У подальшому викладі шкідливі програмні та технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, будуть називатися скорочено – *шкідливі програмні та технічні засоби*. Отже, до предметів злочину, передбаченого ст. 361-1 КК, закон відносить програмні та технічні засоби, які: а) є шкідливими та б) призначені для несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Передбачена в законі ознака *шкідливі* характеризує ці програмні та технічні засоби як такі, використання яких заподіює шкоду інформаційним відносинам, засобом забезпечення яких є комп'ютерна техніка чи мережі електрозв'язку, або створює небезпеку її

заподіяння. Інша ознака – «призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку», указує на їх спеціальне призначення – несанкціоноване втручання в роботу комп'ютерної техніки чи мереж електрозв'язку. На відміну від будь-яких інших комп'ютерних програм та обладнання шкідливі програмні та технічні засоби спеціально розробляються для несанкціонованого втручання, тобто порушення режиму роботи ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Тому під *шкідливими програмними засобами*, призначеними для несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, слід розуміти програми (програмні блоки, програмне забезпечення), розроблені спеціально для несанкціонованого втручання в роботу комп'ютерної техніки або мереж електрозв'язку, використання яких спричиняє або створює загрозу заподіяння шкоди інформаційним відносинам.

Технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку,– це різного роду пристрої, устаткування, розроблені для несанкціонованого втручання в роботу комп'ютерної техніки або мереж електрозв'язку, використання яких спричиняє або створює загрозу заподіяння шкоди інформаційним відносинам.

4.2. Об'єктивна сторона злочину, передбаченого ст. 361-1 Кримінального кодексу України

Злочин, передбачений ч. 1 ст. 361-1 КК, відноситься до злочинів із *формальним* складом, тобто вважається закінченим з моменту вчинення одного з альтернативних діянь, зазначених у диспозиції. Досліджувана норма передбачає такі форми об'єктивної сторони:

– створення шкідливих програмних або технічних засобів з метою використання, розповсюдження або збуту;

– розповсюдження шкідливих програмних або технічних засобів;

– збут шкідливих програмних або технічних засобів.

Створення шкідливих програмних або технічних засобів є результатом діяльності щодо розроблення таких засобів у вигляді нового шкідливого програмного або технічного засобу. Зазначимо, що створення буде кримінально караним тільки за наявності відповідної ознаки суб'єктивної сторони – мети використання, розповсюдження або збуту.

Розповсюдження шкідливих програмних засобів. Важливо зауважити, 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 й іншими способами, а також шляхом продажу, прокату, здавання в найм, надання в позику, а так само 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 мережними й іншими способами, а також шляхом продажу, здавання в найм, надання в позику, включаючи імпорт для будь-якої з 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 (флоппі-дисків, CD-R) або за допомогою модему чи передавання комп'ютерною мережею»[3].

Автори науково-практичного коментаря КК 1961 р., аналізуючи ст. 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 техніч-

[1] Див.: *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] Див.: *Российское* уголовное право. Особенная часть: Учебник / Под ред. М. П. Журавлева, С. И. Никулина.– М.: Спарк, 1998.– С. 339.

[3] Див.: *Уголовное* право России. Особенная часть: Учебник / Под ред. проф. А. И. Рарога.– М.: Ин-т международного права и экономики им. А. С. Грибоедова, 1998.– С. 327.

них засобів, призначених для несанкціонованого доступу до інформації[1].

Викладене дає можливість зробити висновок, що, незважаючи на розходження у визначеннях поняття розповсюдження, усі вони ґрунтуються, по-перше, на традиційному розумінні розповсюдження як надання оплатного або безоплатного доступу до якогось предмета невизначеному колу осіб, а, по-друге, на виділенні специфічних ознак розповсюдження шкідливих програмних засобів, зумовлених особливостями предмета розповсюдження.

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

– самовідтворення;
– «закладання» в програмне забезпечення;
– розповсюдження з використанням комп'ютерної мережі.

Розповсюдження шкідливих програм способом *самовідтворення* означає, що розробник передбачає можливість шкідливої програми створювати свої копії. Цей спосіб найчастіше застосовується для розповсюдження «комп'ютерних вірусів».

Комп'ютерний вірус – це параметр, який проникає в комп'ютерну програму та порушує функціонування комп'ютера, а також здатен самостійно копіювати комп'ютерні команди або заміняти програмні дані[2]. Найяскравішим прикладом комп'ютерного вірусу є так званий вірус Морріса. У листопаді 1988 р. 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 у 98 млн доларів[1].

[1] Див.: *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.

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

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 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 «закладеним» елементом знищуються або перекручуються всі текстові документи на жорсткому диску.

Розповсюдження шляхом використання комп'ютерних мереж полягає, як правило, у наданні доступу до шкідливих програм шляхом їх розміщення на мережевих носіях інформації або у розсилці електронною поштою копій шкідливих програм. Прикладом останнього способу може слугувати механізм розповсюдження одного із відомих вірусів останнього часу I LOVE YOU – «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[2].

Для прикладу розповсюдження шкідливих програм шляхом надання доступу розглянемо вирок Кіровського районного суду м. Кіровограда по справі № 1-57/08 від 16 січня 2009 р.[3] щодо обвинувачення А. у вчиненні злочину, передбаченого ч. 1. ст. 361-1 КК України. Зокрема, у вироку зазначається, що 27 жовтня 2006 р. в 0 год 36 хв А., користуючись локальною комп'ютерною мережею гуртожитків, діючи умисно, скачав, шляхом копіювання, з комп'ю-

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

[2] Див.: *Милкус А.* Скромный компьютерщик опаснее атомной бомбы // Комсомольская правда.– 2000.– 11 мая.– С. 3.

[3] *Вирок* Кіровського районного суду м. Кіровограда по справі № 1-57/08 від 16 січня 2009 р. // Єдиний державний реєстр судових рішень.– Режим доступу: http://www.reyestr.court.gov.ua/

терної адреси, назву якої він не пам'ятає на власний персональний комп'ютер (ноутбук) виробництва HP (Intel Pentium 1.73 Ghz, 1 Gb оперативної пам'яті, жорсткий диск 80 Gb, серійний номер CNF5372F1Y), в папку «Hack» за адресою: C:/Install/For Windows/XP/Hack/, шкідливі програмні засоби, а саме: «Passware Kit v65 Enterprise», «AsterWin», що призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

При цьому, він усвідомлював, що особисто, *шляхом відкриття диску «С» для вільного, безперешкодного доступу до нього у локальній комп'ютерній мережі всім її абонентам, опосередковано пропонує їм в безоплатний спосіб та надає можливість вільного доступу* (курсивом помічено спосіб розповсюдження – авт.), копіювання і використання на власний розсуд шкідливих програмних засобів.

21 травня 2008 р. співробітниками відділу контррозвідки Управління СБ України в Кіровоградській області під час здійснення оперативно-розшукових заходів, спрямованих на перевірку можливого факту розповсюдження або збуту шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку встановлено, що в кімнаті №_, розташовано технічне обладнання під'єднане до локальної комп'ютерної мережі вказаного навчального закладу. При цьому, під час огляду місця події встановлено, що вказане технічне обладнання з'єднано з персональним комп'ютером розміщеним в кімнаті №_ вказаного гуртожитку з IP-адресою: «10.0.0.23» та комп'ютерним ім'ям «Furik», що належить громадянину А., і на ньому за адресою: C:/Install/For Windows/XP/Hack/ розміщено програмне забезпечення, яке було надано для загального доступу, зокрема: «TMeter», «htfilter-07.exe», «NetLook», «Passware Kit v65 Enterprise», «AsterWin», «ipscan», «rsd», «SMAC».

Згідно із висновком експерта № 43 від 24.06.2008 р. комп'ютерне програмне забезпечення «Passware Kit v65 Enterprise» і «AsterWin», яке міститься у папці загального доступу C:/Install/ є програмами для видаленого зчитування паролів або нейтралізації засобів захисту комп'ютерних програм чи інформації та є програмами-шпигунами, які після встановлення паролів та їх нейтралізації надають можливість проникнення до певної комп'ютерної інформації, комп'ютерної програми, комп'ютерної мережі, операційної

системи і непомітно для власника чи законного користувача здійснювати несанкціоновану передачу інформації сторонній особі. Таким чином, суд правильно кваліфікував дії А. за ч. 1 ст. 361-1 КК, як *розповсюдження шкідливих програмних засобів, призначених для несанкціонованого втручання* в роботу комп'ютерної техніки.

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.

Зважаючи на викладене вище, можна дати таке визначення розповсюдження шкідливого програмного забезпечення: *оплатне або безоплатне надання копій шкідливих програм або доступу до них невизначеному колу осіб, а також їх «закладання» в програмне забезпечення або розповсюдження за допомогою комп'ютерних мереж чи поширення шляхом самовідтворення.*

Розповсюдження шкідливих технічних засобів аналогічне простому розповсюдженню матеріальних предметів. Однак і це діяння має певну специфіку. Крім простого передавання таких засобів, можливим є їх установлення в ЕОМ, 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. В окремих випадках 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 в особи, яка розповсюджує шкідливі програмні та технічні засоби за згодою особи, що 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 р. 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 створенні відповідних шкідливих засобів.

Збут шкідливих програмних або технічних засобів відрізняється від розповсюдження тим, що він пов'язаний з відчуженням предмета. Тобто, якщо при розповсюдженні предмет залишається в особи (шкідливе програмне забезпечення продовжує знаходитися на мережевому ресурсі, з якого розповсюджується, повертається шкідливий програмний засіб, що передавався для використання), то в результаті збуту він відчужується, тобто не залишається в особи, яка його збуває. Отже, під збутом шкідливих програмних або технічних засобів слід розуміти *їх оплатне або безоплатне відчуження*. Типовим прикладом збуту шкідливих програм є продаж дисків із записаними на них шкідливими програмами[1].

4.3. Суб'єктивні ознаки створення, розповсюдження або збуту шкідливих програмних або технічних засобів

Суб'єкт даного злочину загальний, ним є фізична, осудна особа, що досягла 16-річного віку.

Оскільки злочин, передбачений ст. 361-1 КК, відноситься до злочинів із формальним складом, зміст його *суб'єктивної сторони* визначається лише психічним ставленням до діяння і полягає в усвідомленні суспільної небезпечності та протиправності створення, розповсюдження або збуту шкідливих програмних або технічних засобів та бажанні вчинення таких дій.

[1] Див.: *Вирок* Рівненського міського суду Рівненської області по справі № 1-738/2007 від 25 жовтня 2007 р. // Єдиний державний реєстр судових рішень.– Режим доступу: http://www.reyestr.court.gov.ua/

Отже, у цій формі умисел може бути тільки прямим, а його специфіка виражається в тому, що свідомістю особи обов'язково охоплюється розуміння того, що створювані або розповсюджувані засоби *спеціально призначені для несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку.*

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, в якому пропонує, наприклад, за винагороду, розповсюджувати цю програму всім, хто її скопіював. У такому разі 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 складового елементу суб'єктивної сторони розповсюдження або збуту 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.

Запитання для самоконтролю та самоперевірки

1. Визначіть шкідливі програмні та технічні засоби як предмет злочину.
2. Як класифікують шкідливі програмні засоби за способом розповсюдження?
3. Яка кримінальна відповідальність за створення шкідливих програмних і технічних засобів?
4. Чим розповсюдження шкідливих програмних або технічних засобів відрізняється від їх збуту?
5. Яка специфіка суб'єктивної сторони створення, розповсюдження або збуту шкідливих програмних і технічних засобів?

Розділ 5. Кримінально-правова охорона комп'ютерної інформації з обмеженим доступом (ст. 361-2 КК України)

Об'єктом злочину – несанкціонованого збуту або розповсюдження інформації з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України), є суспільні відносини власності на комп'ютерну інформацію з обмеженим доступом.

Предметом злочину є інформація з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства. Тобто, інформація, що є предметом злочину, передбаченого ст. 361-2 КК України, характеризується такими ознаками:

– вона відноситься до інформації з обмеженим доступом;

– зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

– створена відповідно до чинного законодавства;

– захищена відповідно до чинного законодавства.

До *інформації з обмеженим доступом* згідно зі ст. 30 Закону України «Про інформацію»[1] відноситься таємна і конфіденційна інформація.

До таємної інформації належать відомості, що становлять державну та іншу *передбачену законом* таємницю, 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 й поставлено під охорону з

[1] Див.: *Закон* України «Про інформацію» від 02.11.1992 р. // Закони України.– Т. 4.– К., 1996.– С. 72–88.

боку держави. Віднесення інформації до державної таємниці та порядок її використання визначаються Законом України «Про державну таємницю» від 21 січня 1994 р[1].

До таємної інформації, крім державної, відноситься також інша передбачена законом таємниця, розголошення якої завдає шкоди особі, суспільству, державі. Такою може бути, наприклад, таємниця страхування[2], таємниця усиновлення, таємниця досудового слідства тощо.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні *окремих фізичних або юридичних осіб* і розповсюджуються *на їх розсуд* і відповідно до передбачених ними умов. Виходячи з аналізу ч. 3 ст. 30 Закону України «Про інформацію»[3], можна залежно від характеру, змісту відомостей, що становлять 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, на підставі ч. 1 ст. 36 Господарського кодексу України, відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, що не є державною таємницею, розголошення яких може завдати шкоди інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею.

Перелік відомостей, що становлять комерційну таємницю підприємства, порядок роботи з ними й організація їх охорони визначаються наказом керівника, зміст якого не повинен суперечити положенням чинного законодавства. Підставою для прийняття такого наказу є згадана норма Господарського кодексу України, в якій зазначається: «Склад і обсяг відомостей, що становлять комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання відповідно до закону». Перелік відомостей, які не можуть становити комерційну таємницю, міститься

[1] Див.: *Закон* України «Про державну таємницю» від 21.01.1994 р. // Закони України.– Т. 7.– К., 1997.– С. 38–50.

[2] Див.: *Стаття* 40 Закону України «Про страхування» від 07.03.1996 р.

[3] Див.: *Закон* України «Про інформацію» від 02.11.1992 р. // Закони України.– Т. 4.– К., 1996.– С. 72–88.

в Постанові Кабінету Міністрів України від 9 серпня 1993 р. № 611 «Про перелік відомостей, які не складають комерційну таємницю».

Використання терміна «інформація, яка зберігається (або оброблюється (ст. 362 КК України) в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або на носіях такої інформації» є не зовсім вдалим, оскільки він є громіздким, а за змістом повністю відповідає більш вдалому термінові «комп'ютерна інформація», що використовувався у попередній редакції розділу XVI КК України. Крім того, навряд чи можна визнати доцільним розмежування термінів «інформація, що оброблюється...» (ст. 362 КК) та «інформація, що зберігається...» (ст. 361-2 КК) оскільки оброблення інформації в ЕОМ, системі чи комп'ютерній мережі обов'язково передбачає її зберігання, а зберігання передбачає оброблення. У цьому питанні можна погодитися з Д. С. Азаровим, який зазначає, що закон має визначати форму подання інформації, а не спосіб або засоби її оброблення чи зберігання[1]. Таким чином, друга виділена нами ознака інформації як предмета злочину, передбаченого ст. 361-2 КК, полягає в тому, що вона є комп'ютерною, тобто подана у формі, що дозволяє її оброблення або зберігання з використанням комп'ютерної техніки.

Інформація, що є предметом даного злочину, *створена відповідно до чинного законодавства*, тобто розповсюдження або збут інформації, отриманої з порушенням законодавства, не є злочином, передбаченим ст. 361-2 КК України.

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31 травня 2005 р. інформація з обмеженим доступом повинна оброблятися із застосуванням *«комплексної системи захисту інформації з підтвердженою відповідністю»* (ч. 2 ст. 8 Закону).

Отже, предметом злочину є та інформація, що зберігається в такій системі; склад злочину, передбачений цією статтею, буде мати місце тоді, коли незаконно розповсюджується або збувається інформація, що зберігається із застосуванням комплексної системи захисту. Ця система є сукупністю організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації. Відповідно до чинного законодавства видачу

[1] Див.: *Азаров Д. С.* Нові зміни до розділу XVI Особливої частини Кримінального кодексу України – нові проблеми // Юридичний вісник України.– 2005.– № 6.– С. 29.

атестатів відповідності комплексних систем захисту інформації здійснює Державна служба спеціального зв'язку та захисту інформації України. До основних завдань цієї служби належать: участь у формуванні та реалізація державної політики у сфері захисту державних інформаційних ресурсів; забезпечення урядового зв'язку; визначення вимог і порядку створення та розвитку систем технічного та криптографічного захисту інформації, яка є власністю держави, здійснення державного контролю за станом криптографічного та технічного захисту такої інформації тощо[1].

За конструкцією *об'єктивної сторони* злочин, передбачений ст. 361-2 КК України, є формальним. Він вважається закінченим з моменту вчинення несанкціонованого збуту або несанкціонованого розповсюдження комп'ютерної інформації з обмеженим доступом.

Збут або розповсюдження інформації буде *несанкціонованим*, коли він вчиняється без дозволу власника цієї інформації.

Розповсюдження комп'ютерної інформації з обмеженим доступом – це оплатне або безоплатне надання копій цієї інформації або доступу до неї невизначеному колу осіб. Одним із прикладів даного діяння є незаконне розповсюдження персональних даних. Так, у 2003 р. в продажу з'явилася база даних абонентів одного з лідерів російського ринку операторів стільникового зв'язку «Мобільні ТелеСистеми» (МТС). База даних містила такі персональні дані про абонентів компанії, як прізвище, ім'я, по батькові, дата народження, паспортні дані, індивідуальний номер платника податків тощо. При цьому інформація про появу такої бази даних за кілька тижнів розповсюджувалася в Інтернеті[2].

Під *збутом комп'ютерної інформації з обмеженим доступом* необхідно розуміти її оплатне або безоплатне відчуження.

Суб'єкт злочину – загальний. Якщо збут або розповсюдження інформації з обмеженим доступом вчиняє особа, якій інформацію було довірено у зв'язку з виконанням службових або професійних обов'язків, вчинене, за наявності відповідних ознак суб'єктивної сторони, необхідно кваліфікувати за ст. 232 або ст. 328 КК України. Більш докладно питання відмежування злочину, передбаченого ст. 361-2 КК України, розглядаються в розділі VIII.

[1] *Закон* України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 р.

[2] Див.: *Михеева М. Р.* Проблема правовой защиты персональных данных.– Режим доступа: http://www.crime.vl.ru/doc/stats/stat_93.html

Суб'єктивна сторона даного злочину характеризується виною у формі прямого умислу: особа усвідомлює суспільну небезпечність і протиправність збуту або розповсюдження комп'ютерної інформації з обмеженим доступом та бажає вчиняти такі дії. Особа усвідомлює, що комп'ютерна інформація, яку вона збуває або розповсюджує, є інформацією з обмеженим доступом; усвідомлює, що не має права або дозволу власника інформації на вчинення подібних дій.

Запитання для самоконтролю та самоперевірки

1. Що таке «інформація з обмеженим доступом»?
2. Визначіть зміст і розмежування понять «таємна інформація» та «конфіденційна інформація».
3. Назвіть особливості автоматизованого опрацювання інформації з обмеженим доступом.
4. Чим збут інформації з обмеженим доступом відрізняється від її розповсюдження?
5. Охарактеризуйте суб'єктивну сторону складу злочину, передбаченого ст. 361-2 КК України.

Розділ 6. Комп'ютерні злочини, що вчиняються особами, які наділені певними правами щодо доступу до інформації або використання електронно-обчислювальних машин, систем і мереж електрозв'язку (статті 362 та 363 КК України

6.1. Кримінальна відповідальність за незаконні дії з комп'ютерною інформацією, вчинені особою, яка має право доступу до неї

У літературі досить поширеною є така класифікація суб'єктів незаконного втручання: а) особи, які перебувають у трудових відносинах з підприємством, організацією, установою, фірмою чи компанією, в якій вчинено злочин (особи, які безпосередньо займаються обслуговуванням ЕОМ: оператори, програмісти, інженери, персонал, який займається технічним обслуговуванням і ремонтом комп'ютерної техніки); користувачі ЕОМ, які мають певну підготовку та вільний доступ до комп'ютерної системи; адміністративно-керівний персонал (керівники, бухгалтери, економісти); б) особи, які не перебувають у трудових відносинах з підприємством, організацією, установою, фірмою чи компанією, в якій вчинено злочин[1]. Як свід-

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

чить практика зарубіжних правоохоронних органів, досить часто комп'ютерні злочини 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 ЕОМ, 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[1]. 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[2].

Про те, що більшість злочинів у сфері використання ЕОМ, систем і 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%»[3].

Таким чином, практика боротьби з комп'ютерними злочинами свідчить про підвищену небезпечність цих злочинів у випадку їх вчинення особою, яка має право доступу до інформації, що є предметом посягання. Саме це й зумовило наявність у КК України ст. 362, яка передбачає відповідальність спеціального суб'єкта за незаконні дії з комп'ютерною інформацією.

Об'єктом даного злочину є суспільні відносини власності на комп'ютерну інформацію. *Предметом* злочину відповідно до диспозиції є інформація, яка опрацьовується в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації. Як уже зазначалося, термін, що вживається для характеристики предмета, є не зовсім вдалим: він громіздкий, а за змістом не відрізняється від більш вдалого – «комп'ютерна інформація». Отже, предметом даного злочину є комп'ютерна інформація, ознаки якої розглядалися вище.

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

[2] Див.: *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/1030anal.html

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

Об'єктивна сторона даного злочину характеризується наявністю декількох форм:

– несанкціонована зміна комп'ютерної інформації;

– несанкціоноване знищення комп'ютерної інформації;

– несанкціоноване блокування комп'ютерної інформації;

– несанкціоноване перехоплення комп'ютерної інформації, що призвело до її витоку;

– несанкціоноване копіювання комп'ютерної інформації, що призвело до її витоку.

Несанкціонована зміна комп'ютерної інформації є порушенням права власності на інформацію шляхом перекручення без відома власника змісту відомостей, відображених на носії, що робить інформацію, цілком або частково непридатною для задоволення інформаційної потреби особою, яка має право власності на таку інформацію.

Несанкціоноване знищення комп'ютерної інформації має місце тоді, коли вона перестає існувати у формі, яка дозволяє її опрацювання за допомогою комп'ютерної техніки.

Несанкціоноване блокування комп'ютерної інформації – позбавлення власника можливості використовувати інформацію для задоволення інформаційної потреби за умови, що її не втрачено та не підроблено.

Якщо три перші форми є простими, звичайними злочинами з матеріальним складом і вважаються закінченими з моменту настання зазначених наслідків, то структура двох останніх – несанкціонованого перехоплення та копіювання – ускладнена наявністю віддаленого наслідку – витоку інформації, якому передують таки види порушення права власності на комп'ютерну інформацію як несанкціоноване копіювання або перехоплення.

Оскільки *витік інформації* відповідно до ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31 травня 2005 р. є результатом дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що *не мають права доступу до неї*, можна зробити висновок, що предметом несанкціонованого перехоплення

або копіювання є тільки комп'ютерна інформація з обмеженим доступом (таємна або конфіденційна).

Копіювання комп'ютерної інформації – це «відтворення даних зі збереженням вихідної інформації»[1]. Відповідно несанкціоноване копіювання можна визначити як відтворення, з перевищенням наданих власником прав доступу, комп'ютерної інформації з обмеженим доступом зі збереженням вихідної інформації. Наприклад, особа має право лише на ознайомлення та внесення змін до певної бази даних, а вона, без дозволу власника, створює її копію.

Перехоплення – специфічний вид копіювання. Його особливість полягає в способі отримання копії. Відповідно до Конвенції про кіберзлочинність, прийнятої в рамках Ради Європи 23 листопада 2001 р. (ратифікована Україною у вересні 2005 р.), *несанкціонованим перехопленням* є навмисне перехоплення технічними засобами, без права на це, передавання комп'ютерних даних, не призначених для публічного користування, які проводяться з комп'ютерної системи, усередині її або на неї, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані.

Отже, несанкціоноване перехоплення: 1) вчиняється за допомогою специфічних технічних засобів; 2) полягає в отриманні копії інформації під час її передавання від одного комп'ютера до іншого, або від периферійних приладів до комп'ютера, або шляхом обробки електромагнітних випромінювань під час роботи ЕОМ, автоматизованих систем або комп'ютерних мереж; 3) особа, що вчиняє перехоплення, не має права на отримання інформації з обмеженим доступом, що є його предметом. Таким чином, *несанкціоноване перехоплення* – це отримання, з перевищенням наданих власником прав, копії інформації з обмеженим доступом за допомогою специфічних технічних засобів під час передавання цієї інформації від одного комп'ютера до іншого, або від периферійних приладів до комп'ютера, або шляхом обробки електромагнітних випромінювань під час роботи ЕОМ, автоматизованих систем або комп'ютерних мереж, в яких опрацьовується така інформація.

Наприклад, під час роботи ЕОМ сигнали, які формують зображення на дисплеї, можуть за допомогою спеціального обладнання отримуватися на певній відстані від працюючого комп'ютера. Таким чином, особа шляхом перехоплення отримуватиме ту комп'ютерну інформацію, яка відображається на дисплеї.

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

Суб'єкт злочину, передбаченого ст. 362 КК, спеціальний – особа, яка має право доступу до комп'ютерної інформації. Такий статус особи встановлюється відповідним наказом або розпорядженням власника інформації.

Суб'єктивна сторона даного злочину характеризується виною у формі прямого або непрямого умислу: особа усвідомлює суспільну небезпечність і протиправність своїх дій і бажає або свідомо допускає настання наслідків. При цьому особа має усвідомлювати, що вчиняє такі дії, які є перевищенням повноважень, наданих власником інформації.

Достатньо цікавий приклад злочину, що розглядається, описується у вироку Косівського районного суду Івано-Франківської області по справі № 1-56/2007 від 7 червня 2007 р.[1] щодо обвинувачення Б. у вчиненні злочинів, передбачених статтями 364, 366 та 362 КК України. Так, Б. працював з 3 грудня 2001 р. до 25 квітня 2006 р. на посаді бухгалтера з реалізації філії ВАТ «Прикарпаттяобленерго» Косівського РЕМ та був *особою, яка має доступ до програми, призначеної для комп'ютерної обробки інформації* щодо розрахунків з юридичними споживачами (характеристика спеціального суб'єкта – *авт.*).

Приватне підприємство «Фірма Явсон» згідно договору на постачання електроенергії № 00109/1 від 28 квітня 2004 р. протягом червня 2004 р.– лютого 2006 р. оплатила за використану електроенергію 382 671,45 грн. У цей час, Б., зловживаючи своїм службовим становищем, діючи умисно, в інтересах третіх осіб, а саме приватних підприємців Т., Р., Л., В., Д. протягом вказаного періоду часу незаконно занизив показник спожитої електроенергії ПП «Фірма Явсон» та коштів фактично сплачених за неї в сумі 76 008,07 грн., які безпідставно, у програмі розрахунків з юридичними споживачами, розніс вказаним приватним підприємцям, що споживали електроенергію, але не здійснювали оплати за неї. Внаслідок цих умисних дій ВАТ «Прикарпаттяобленерго» заподіяно тяжкі наслідки в сумі 76 008,07 грн., які в 250 разів перевищують неоподаткований мінімум доходів громадян.

Суд правильно кваліфікував дії Б., що виразились у зловживанні службовим становищем, тобто умисному, в інтересах третіх

[1] *Вирок* Косівського районного суду Івано-Франківської області по справі № 1-56/2007 від 7 червня 2007 р. // Єдиний державний реєстр судових рішень.– Режим доступу: http://www.reyestr.court.gov.ua/

осіб використанні свого службового становища всупереч інтересам служби, що заподіяло тяжкі наслідки як злочин, передбачений ч. 2 ст. 364 КК України. Крім цього, правильною є й оцінка дій підсудного за ст. 366, як службового підроблення, та ст. 362, як *несанкціонованої зміни комп'ютерної інформації, вчиненої особою, яка має доступ до неї.* Зазначимо, що в даному випадку вчинене Б. службове підроблення обов'язково потребувало додаткової кваліфікації за ст. 362, оскільки спосіб, в який вчинено службове підроблення, є самостійним злочином (ст. 362), який не охоплюється диспозицією відповідної норми про злочин у сфері службової діяльності.

6.2. Кримінальна відповідальність за порушення правил експлуатації комп'ютерної техніки чи мереж електрозв'язку та за порушення порядку чи правил захисту інформації, яка в них оброблюється

Кримінальну відповідальність за порушення правил експлуатації комп'ютерних засобів оброблення інформації та мереж електрозв'язку, а також порушення порядку чи правил захисту інформації встановлено в ст. 363 КК України «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється».

Об'єкт злочину, передбаченого цією статтею, становлять суспільні відносини, у межах яких забезпечується безпека використання ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також дотримання порядку та правил захисту комп'ютерної інформації.

Диспозиція даної статті є бланкетною, тобто містить посилання на інші нормативно-правові акти. Але, на жаль, на сьогодні не можна сказати, що законодавство про безпеку експлуатації комп'ютерної техніки, мереж електрозв'язку та захист комп'ютерної інформації достатньо розвинене. Саме тому воно не містить окремих нормативно-правових актів, які чітко визначали б правила

експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, порядок і правила захисту комп'ютерної інформації.

Правила експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку вміщують вимоги, що ставляться власником ЕОМ, автоматизованої системи, комп'ютерної мережі або мережі електрозв'язку до їх використання або обслуговування цих технічних засобів. Вони, як правило, містяться в окремих підзаконних актах (наказах, розпорядженнях), що видаються власником комп'ютерної техніки або мережі електрозв'язку. Наприклад, правила експлуатації засобів обчислювальної техніки в Міністерстві фінансів України регламентуються Наказом міністра фінансів України № 248 від 1 квітня 2003 р. «Про затвердження Положення про роботу із засобами обчислювальної техніки та про доступ до інформаційних ресурсів Міністерства фінансів України». Цим наказом користувачам заборонено розкривати корпуси засобів обчислювальної техніки, вносити зміни до конфігурації або самостійно їх ремонтувати; під'єднання засобу обчислювальної техніки користувача до телекомунікаційної мережі, установлення, оновлення та вилучення програмного забезпечення здійснюють відповідні спеціалісти та ін.

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31 травня 2005 р. захист інформації в системі – це діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі. Регламентація цієї діяльності здійснюється за допомогою визначення порядку та правил захисту комп'ютерної інформації. Видається, що *порядок захисту інформації* – це визначені нормативно-правовими актами вимоги щодо створення системи захисту інформації та організації її роботи. *Правила захисту інформації*, у свою чергу, є вимогами щодо використання системи захисту інформації певного інформаційного ресурсу. Тобто, якщо систему захисту певного інформаційного ресурсу не створено, то й неможливо порушити правила захисту цього ресурсу. Той факт, що систему захисту не створено, може бути визнаний, за наявності відповідних нормативно-правових положень, порушенням порядку захисту інформації.

На певну увагу заслуговують питання нормативної регуляції захисту комп'ютерної інформації. Зазначимо, що вони вирішуються практично на всіх рівнях: прийнято відповідні закони, їх положення конкретизуються указами Президента, рішеннями Кабінету Міністрів, нормативними документами міністерств і відомств.

Базовим нормативним документом у сфері захисту комп'ютерної інформації є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31 травня 2005 р. У цьому законі формулюється, можна сказати, головний принцип регулювання питань захисту комп'ютерної інформації національним законодавством: *відповідальність за захист інформації покладається на власника системи (в якій вона обробляється), при цьому в тих випадках, коли в системі обробляється інформація, що є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, вона повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю.* Тобто, спеціальні вимоги встановлюються лише до захисту державної інформації або інформації, захист якої спеціально передбачено в законі. Решта нормативних актів у сфері інформаційної безпеки конкретизує це положення.

Так, правові та організаційні засади технічного захисту інформації органів державної влади, органів місцевого самоврядування, органів управління Збройних Сил України й інших військових формувань, утворених згідно із законодавством України, відповідних підприємств, установ, організацій установлюються Указом Президента України «Про Положення про технічний захист інформації в Україні» від 27 вересня 1999 р. Також указом Президента створюється відповідний орган державного управління – Департамент спеціальних телекомунікаційних систем та захисту інформації, що діє в складі Служби безпеки України. Цей департамент «реалізовує державну політику у сфері захисту державних інформаційних ресурсів у мережах передачі даних, криптографічного та технічного захисту інформації, забезпечує функціонування державної системи урядового зв'язку»[1], саме цей департамент, до речі, проводить сертифікацію засобів технічного захисту інформації.

Постановами Кабінету Міністрів України встановлюються чіткі вимоги щодо інформаційної безпеки в органах державної влади. Так, відповідними постановами уряду як обов'язкова складова державних автоматизованих інформаційних систем передбачається

[1] *Указ* Президента України «Питання Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України» від 6 жовтня 2000 р.

ся система захисту інформації[1]; на органи державної влади покладається вимога щодо забезпечення захисту інформаційного наповнення їх веб-порталів[2]; спеціальні вимоги щодо інформаційної безпеки ставляться до програмного забезпечення, яке використовується державними органами[3], та до провайдерів, котрі надають послуги доступу до мережі Інтернет органам державної влади[4], тощо.

У свою чергу, нормативними документами міністерств і відомств закріплюються конкретні організаційні та інженерно-технічні заходи безпеки щодо їх інформаційних ресурсів. Наприклад, Інструкцією Національного банку України про безготівкові розрахунки в Україні в національній валюті[5] передбачено такий організаційний захід: якщо під час використання систем «клієнт – банк», «клієнт – Інтернет – банк» клієнт не дотримується вимог, що встановлює банк, з питань безпеки опрацювання електронних розрахункових документів, банк має право припинити обслуговування клієнта за допомогою системи. Мають місце й такі організаційні заходи, як установлення інструкцій щодо використання відомчих

[1] Див.: *Постанова* Кабінету Міністрів України «Про заходи щодо створення електронної інформаційної системи «Електронний Уряд» від 24 лютого 2003 р.; Постанова Кабінету Міністрів України «Про Єдину державну інформаційну систему у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, і фінансуванню тероризму» від 10 грудня 2003 р.; Постанова Кабінету Міністрів України «Про державну комп'ютеризовану систему моніторингу сплати податків, зборів (обов'язкових платежів)» від 25 серпня 2004 р.; Постанова Кабінету Міністрів України «Про затвердження Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління» 3 серпня 2005 р.

[2] Див.: *Постанова* Кабінету Міністрів України «Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади» від 4 січня 2002 р.

[3] Див.: *Постанова* Кабінету Міністрів України «Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади» від 10 вересня 2003 р.

[4] Див.: *Постанова* Кабінету Міністрів України «Про затвердження Порядку підключення до глобальних мереж передачі даних» від 12 квітня 2002 р.

[5] Див.: *Постанова* Національного банку України «Про затвердження Інструкції про безготівкові розрахунки в Україні в національній валюті» від 21 січня 2004 р.

мереж[1], періодичне створення комісій з перевірки дотримання вимог інформаційної безпеки[2] й навіть обмеження доступу до приміщень, в яких розташоване обладнання, що забезпечує роботу мережі[3]. До технічних заходів, передбачених відомчими нормативними документами, можна віднести: обов'язкове включення до відомчих комп'ютерних мереж засобів технічного захисту інформації[4] та встановлення відповідних вимог до обладнання та програмного забезпечення[5].

Спеціальних вимог щодо захисту комп'ютерної інформації, яка не є власністю держави, крім положення Закону України «Про захист інформації в автоматизованих системах», що захист інформації покладається на власника системи, національне законодавство не встановлює. Тому порушення правил експлуатації ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електро-

[1] Див.: *Наказ* Міністерства фінансів України «Про затвердження Положення про роботу із засобами обчислювальної техніки та про доступ до інформаційних ресурсів Міністерства фінансів України» від 1 квітня 2003 р.; Наказ Міністерства економіки та з питань європейської інтеграції України «Про заходи щодо захисту конфіденційної і відкритої інформації, що циркулює в автоматизованій системі Міністерства» від 23 квітня 2002 р.

[2] Див.: *Наказ* Міністерства аграрної політики України «Про організацію роботи з технічного захисту інформації в Міністерстві аграрної політики України» від 16 серпня 2000 р.; Наказ Міністерства аграрної політики України «Про організаційні заходи щодо захисту інформації з обмеженим доступом» від 11 грудня 2002 р.

[3] Див.: *Наказ* Міністерства фінансів України «Про забезпечення захисту інформації шляхом обмеження доступу до приміщень, в яких розміщене серверне та комутаційне обладнання» від 20 липня 2004 р.

[4] Див.: *Постанова* Правління Пенсійного фонду України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, в Пенсійному фонді України та його органах» від 27 червня 2002 р.; Постанова Правління Фонду соціального страхування від нещасних випадків на виробництві та професійних захворювань України № 55 від 29 липня 2004 р. «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, у виконавчій дирекції Фонду соціального страхування від нещасних випадків на виробництві та професійних захворювань України і її робочих органах».

[5] Див.: *Розпорядження* Державної комісії з регулювання ринків фінансових послуг України № 4122 від 3 червня 2005 р. «Про затвердження Вимог до програмного забезпечення та спеціального технічного обладнання кредитних спілок, пов'язаного з наданням фінансових послуг».

зв'язку, в яких обробляється недержавна інформація, стосовно якої законодавство не встановлює спеціальних вимог щодо забезпечення її захисту, а також порушення порядку чи правил захисту такої інформації, якщо воно заподіяло істотну шкоду, буде вважитися злочином, передбаченим ст. 363 КК України, лише тоді, коли власником інформації або власником засобу автоматизованого опрацювання інформації у формі наказу, розпорядження або іншого офіційного документа закріплено відповідні правила експлуатації, порядок і правила захисту інформації.

Склад злочину, передбаченого даною статтею, матеріальний, отже, його *об'єктивна сторона* характеризується такими ознаками:

– діяння – порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту комп'ютерної інформації;

– суспільно небезпечні наслідки – значна шкода;

– причиновий зв'язок між діянням і суспільно небезпечними наслідками.

Аналіз диспозиції дає можливість зробити висновок про те, що діяння може виявлятися у трьох альтернативних формах:

– порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

– порушення порядку захисту комп'ютерної інформації;

– порушення правил захисту комп'ютерної інформації.

Порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – недотримання вимог, що ставляться власником ЕОМ, автоматизованої системи, комп'ютерної мережі або мережі електрозв'язку, до їх використання або обслуговування. Таке порушення може полягати, наприклад, у спробі користувача самостійно встановлювати нове програмне або апаратне забезпечення, підключенні комп'ютерної техніки до електромережі без фільтрів, порушенні порядку включення або відключення засобів комп'ютерної техніки тощо.

Порушення порядку захисту комп'ютерної інформації – недотримання визначених нормативними актами вимог щодо створення системи захисту інформації та організації її роботи. Прикладом такого діяння може бути використання комп'ютерної техніки для роботи з таємною інформацією за відсутності сертифікованої належним чином системи захисту.

Порушення правил захисту комп'ютерної інформації – недотримання вимог щодо використання системи захисту інформації певного інформаційного ресурсу. Це може бути, наприклад, неналежне зберігання паролів для доступу до інформації.

Оскільки аналізований склад злочину є матеріальним, він буде вважатися закінченим від моменту настання суспільно небезпечних наслідків – значної шкоди[1].

Суб'єкт злочину, передбаченого ст. 363 КК, спеціальний – особа, яка відповідає за експлуатацію ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Такий статус особи встановлюється відповідним наказом або розпорядженням власника інформації чи засобу її автоматизованого опрацювання та закріпленими на підставі цього наказу функціональними обов'язками.

Суб'єктивна сторона даного злочину характеризується тим, що діяння може бути вчинене як умисно, так і з необережності, а стосовно наслідків завжди має бути необережність. Якщо настання наслідків охоплюється умислом винної особи, то склад злочину, передбачений ст. 363 КК України, відсутній. У таких випадках дії винної особи, за наявності відповідних ознак, необхідно кваліфікувати як умисне пошкодження майна (ст. 194 КК), або як пособництво в несанкціонованому втручанні в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ч. 5 ст. 27, ст. 361 КК), або як несанкціоновані дії з комп'ютерною інформацією, вчинені особою, що має доступ до неї (ст. 362 КК).

Запитання для самоконтролю та самоперевірки

1. Чим копіювання комп'ютерної інформації відрізняється від її перехоплення?
2. Коли особа, що має право доступу до комп'ютерної інформації, є суб'єктом злочину?
3. Чим порядок захисту комп'ютерної інформації відрізняється від правил її захисту?
4. Назвіть специфічні риси суб'єктивної сторони складу злочину, передбаченого ст. 363 КК України.

[1] Зміст поняття істотна шкода, стосовно комп'ютерних злочинів, було охарактеризовано в підрозділі 2.3 «Кваліфікуючі ознаки комп'ютерних злочинів».

Розділ 7. Кримінальна відповідальність за масове розповсюдження повідомлень електрозв'язку (аналіз складу злочину, передбаченого ст. 363-1 КК України)

Об'єкт перешкоджання роботі ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку через масове розповсюдження повідомлень електрозв'язку злочину становлять суспільні відносини щодо забезпечення безвідмовного функціонування комп'ютерної техніки та мереж електрозв'язку як технічних засобів забезпечення відносин власності на інформацію.

Предметом цього злочину є повідомлення електрозв'язку – відомості, подані у вигляді, що дозволяє їх передавати за допомогою комп'ютерних мереж або мереж електрозв'язку.

Оскільки склад злочину, передбачений ст. 363-1 КК, є *матеріальним*, до ознак його об'єктивної сторони належать: 1) діяння – масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів; 2) суспільно небезпечні наслідки – порушення або припинення роботи ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; 3) причиновий зв'язок між діянням та наслідками.

Отже, діяння як ознака об'єктивної сторони цього складу злочину полягає в розповсюдженні повідомлень електрозв'язку, тобто направленні певним адресатам копій даних повідомлень, яке, по-перше, є масовим і, по-друге, здійснюється без попередньої згоди адресатів.

Розповсюдження слід вважати *масовим* тоді, коли одне або кілька повідомлень отримує більше ніж один адресат, адже в диспозиції аналізованої статті мова йде про множинність повідомлень електрозв'язку та їх адресатів. Зазначимо, що поняття «масове» в даній нормі використовується як оцінне, тобто встановлення того,

чи було певне розповсюдження повідомлень електрозв'язку масовим, залежить від аналізу багатьох обставин конкретного розповсюдження (кількість повідомлень або копій повідомлень, їх розмір; кількість адресатів; час, що було використано для розповсюдження; технічні характеристики обладнання, яке використовувалося для розповсюдження, тощо).

Відсутність попередньої згоди адресатів полягає в тому, що адресат ні в якій формі (письмово, усно, шляхом використання електронної пошти або в інший спосіб) не давав згоди на надсилання йому повідомлень, що є предметом злочину.

Порушення роботи ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, є такою зміною режиму роботи комп'ютерної техніки або мережі електрозв'язку, яка створює загрозу для їх функціонування, тобто погіршення роботи повністю або частково, тимчасове створення перешкод для використання за призначенням.

Припинення роботи ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку полягає в тимчасовому або остаточному припиненні функціонування комп'ютерної техніки або мереж електрозв'язку, невиконанні ними завдань щодо зберігання, опрацювання, пересилання чи отримання комп'ютерної інформації або інформації, що передається мережами електрозв'язку.

Суб'єкт даного злочину загальний.

Суб'єктивна сторона характеризується виною у формі прямого умислу стосовно діяння й умисним або необережним ставленням до наслідків. Особа усвідомлює, що вчиняє масове розповсюдження повідомлень електрозв'язку, і бажає вчиняти такі дії, а також вона бажає або свідомо допускає порушення чи припинення роботи комп'ютерної техніки чи мереж електрозв'язку або легковажно розраховує на ненастання таких наслідків.

Як приклад злочину, передбаченого даною статтею, можна навести випадок, що мав місце у 2004 р. в м. Челябінську (РФ). Основні обставини цього випадку такі[1]. А. створив комп'ютерну програму для масового розсилання коротких текстових повідомлень (SMS-повідомлень) на сайт ЗАТ «Уральський Джи Ес Ем» і через нього на машинні носії абонентів, яке призводило до несанкціонованого блокування інформації та порушення роботи комп'ютерної мережі. Після цього, усвідомлюючи, що використання програми спричинить блокування інформації та порушення роботи комп'ютерної мережі, привів її в дію. У результаті 23 травня 2003 р., у період від 0 год 29 хв до 2 год 46 хв, абоненти Челябінського фрагмента мережі «Мегафон» ЗАТ «Уральський Джи Ес Ем» кількістю 11 261 особа отримали SMS-повідомлення нецензурного змісту, що мало наслідками: 1) порушення роботи комп'ютерної мережі ЗАТ «Уральський Джи Ес Ем», тобто створення аварійної ситуації, що класифікується, відповідно до чинної Інструкції про порядок дій інженера групи оперативно-технічного управління в аварійних ситуаціях, як подія першої категорії «аварія» (подія, яка призводить до погіршення роботи мережі в цілому або її окремих дільниць, у результаті перевантаження обладнання, спричиненого пересиланням надто великого обсягу інформації, та тимчасового створення перешкод для її функціонування відповідно до призначення); 2) блокування комп'ютерної інформації, тобто позбавлення абонентів мережі «Мегафон» ЗАТ «Уральський Джи Ес Ем» можливості приймати та надсилати інші SMS-повідомлення в зазначений період. Такі дії А. повторив і 24 травня 2003 р.

На підставі КК України їх можна було б кваліфікувати за сукупністю злочинів, як: 1) створення з метою використання шкідливої комп'ютерної програми, призначеної для несанкціонованого втручання в роботу комп'ютерної мережі (ст. 361-1 КК); 2) несанкціоноване втручання в роботу комп'ютерної мережі, що призвело до блокування комп'ютерної інформації (ст. 361 КК); 3) масове розповсюдження повідомлень електрозв'язку, що призвело до порушення роботи комп'ютерної мережі (ст. 363-1 КК).

Запитання для самоконтролю та самоперевірки

1. Назвіть об'єктивні ознаки масового розповсюдження повідомлень електрозв'язку.

2. Розмежуйте значення *порушення* роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку від *припинення* їх роботи.

[1] Наводиться за матеріалами сайту «Інтернет і право» (приватний ресурс Антона Серго).– Режим доступу: www.internet-law.ru/intlaw/spam/spamer.htm

Розділ 8. Відмежування комп'ютерних злочинів від суміжних правопорушень

Правильна правова оцінка вчиненого злочину потребує не тільки зіставлення фактичних обставин вчиненого з юридичними ознаками конкретного складу злочину, але й відмежування його від інших, суміжних за деякими ознаками, складів злочинів[1]. Визначення критеріїв розмежування комп'ютерних злочинів між собою та ознак, що дають можливість відмежувати дані суспільно небезпечні діяння від інших злочинних посягань, пов'язаних із використанням комп'ютерної техніки, надасть змогу глибше проаналізувати зміст ознак досліджуваних злочинів, сприятиме їх правильній кваліфікації.

8.1. Розмежування комп'ютерних злочинів

1. Склади злочинів, передбачені статтями 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), 361-1 (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) та 362 (несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї) КК України характеризуються однаковим безпосереднім об'єктом. Цей об'єкт становлять суспільні відносини, у межах яких реалізується право власності на комп'ютерну інформацію, а також суспільні відносини, пов'язані з

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

наданням та отриманням послуг електрозв'язку (статті 361 та 361-1 КК). Водночас ці склади злочинів розрізняються за ознаками предмета. Так, предметом злочину, передбаченого ст. 361 КК, є комп'ютерна інформація та інформація, що передається мережами електрозв'язку, а злочину, передбаченого ст. 362 КК,– тільки комп'ютерна інформація. До предмета злочину, передбаченого ст. 361-1 КК, відносяться шкідливі програмні та технічні засоби. Різною є й конструкція об'єктивної сторони: посягання, передбачені статтями 361 та 362 КК, відносяться до злочинів з матеріальним складом, а ч.1 ст. 361-1 – до злочинів із формальним складом. Розмежовувати дані склади злочинів можна й за ознаками суб'єкта: у складах злочинів, передбачених статтями 361 та 361-1 КК, він загальний, водночас як суб'єкт злочину, передбаченого ст. 362 КК, спеціальний – особа, що має доступ до комп'ютерної інформації.

Однак головною ознакою, що дає можливість розмежувати злочини, передбачені статтями 361 та 362 КК, від злочину, передбаченого ст. 361-1, є, як видається, механізм заподіяння шкоди об'єктові – суспільним відносинам права власності на комп'ютерну інформацію: якщо статті 361 та 362 КК передбачають відповідальність за певні дії, що призводять до заподіяння шкоди предмету цих відносин, чим урешті-решт і заподіюється шкода об'єкту, то ст. 361-1 КК передбачає відповідальність за дії, що створюють небезпеку заподіяння шкоди даним суспільним відносинам. У зв'язку з цим зазначимо, що використання під час вчинення передбаченого ст. 361 або ст. 362 КК злочину шкідливого програмного або технічного засобу, створеного суб'єктом раніше, потребує додаткової кваліфікації за ст. 361-1 КК як створення шкідливого програмного або технічного засобу з метою його використання.

2. Злочини, передбачені ст. 361-2 (несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) та ч. 2 ст. 362 КК України, є посяганням на суспільні відносини власності на комп'ютерну інформацію з обмеженим доступом і характеризуються тим, що їх предметом може бути тільки така комп'ютерна інформація. Між собою вони розрізняються за конструкцією об'єктивної сторони: перший відноситься до злочинів із формальним складом, другий – з матеріальним. Різним є й зміст дій суб'єкта. Злочин, передбачений ст. 361-2 КК, полягає в збуті або розповсюдженні комп'ютерної

інформації, а ч. 2 ст. 362 КК передбачено відповідальність за перехоплення або копіювання такої інформації.

3. Злочин, передбачений ст. 363 КК (порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється), відрізняється від інших посягань, передбачених розділом XVI КК України, практично всіма ознаками складу. Безпосереднім об'єктом більшості складів «комп'ютерних» злочинів є право власності на комп'ютерну інформацію, а злочин, передбачений ст. 363 КК, завдає шкоди відносинам щодо забезпечення встановленого порядку експлуатації комп'ютерної техніки, мереж електрозв'язку, а також порядку та правил захисту інформації.

Диспозиція ст. 363 КК є єдиною бланкетною диспозицією в згаданому розділі, тобто тільки в даному складі злочину діяння полягає в порушенні правил експлуатації комп'ютерної техніки, мереж електрозв'язку або порядку чи правил захисту інформації, передбачених певними нормативно-правовими актами. Спеціальним є й суб'єкт злочину даного злочину – особа, що відповідає за експлуатацію комп'ютерної техніки або мережі електрозв'язку. Суб'єктивна сторона цього злочину характеризується змішаною формою вини: стосовно порушення правил (діяння) можливий як умисел, так і необережність, а щодо настання істотної шкоди (наслідків) – тільки необережність. Якщо ж особа умисно порушує правила експлуатації комп'ютерної техніки або порядок чи правила захисту інформації і до настання зазначених наслідків вона ставиться також свідомо, ознаки складу злочину, передбаченого ст. 363 КК, відсутні. Залежно від обставин справи такі дії можна кваліфікувати як несанкціоновані дії з комп'ютерною інформацією, вчинені особою, що має право доступу до неї (ст. 362 КК), або пособництво у несанкціонованому втручанні в роботу комп'ютерної техніки чи мереж електрозв'язку (ч. 5 ст. 27, ст. 361 КК).

4. Специфіка складу злочину, передбаченого ст. 363-1 КК (перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку), полягає перш за все в ознаках об'єкта. Дана норма, як ми зазначали, захищає суспільні відносини щодо забезпечення безвідмовного функціонування технічних засобів інформаційної діяльності, тимчасом як більшість інших норм аналізованого розділу (усі, крім ст. 363 КК) забезпечують кримінально-правову охорону відносинам власності на комп'ютерну інформацію, тобто певному виду інформаційної діяльності. Тому, якщо масове розсилання повідомлень електрозв'язку призводить, наприклад, до блокування комп'ютерної інформації, а функціонування засобів автоматизованого опрацювання інформації не порушено, ознаки складу злочину, передбаченого ст. 363-1 КК, відсутні. Такі дії можна, за наявності відповідних ознак, кваліфікувати як несанкціоноване втручання (ст. 361 КК), адже шкоду в такій ситуації заподіяно тільки відносинам власності на комп'ютерну інформацію. Водночас, якщо особа здійснила, наприклад, масове розповсюдження комп'ютерної інформації з обмеженим доступом, що, унаслідок надмірного перевантаження, призвело до порушення роботи комп'ютерної мережі, має місце ідеальна сукупність злочинів, передбачених статтями 361-2 та 363-1 КК. У цій ситуації шкода заподіюється і відносинам власності на комп'ютерну інформацію з обмеженим доступом, і відносинам щодо забезпечення безвідмовного функціонування технічних засобів інформаційної діяльності.

8.2. Відмежування комп'ютерних злочинів від інших злочинних посягань, пов'язаних із використанням комп'ютерної техніки

1. З огляду на те, що безпосереднім об'єктом багатьох комп'ютерних злочинів є право власності на комп'ютерну інформацію, необхідно постає проблема їх відмежування від злочинів проти власності, передбачених *главою VI КК України.*

За змістом таких наслідків, як втрата та знищення комп'ютерної інформації, склади злочинів, передбачені статтями 361 та 362 КК, подібні до такого злочину проти власності, як умисне знищення або пошкодження майна: діяння в цих складах 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.

Тому основні відмінності таких складів слід шукати в ознаках об'єкта і 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 згаданих комп'ютерних злочинів є право власності на інформацію. Відмінність цих 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 раніше, 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 і предмета зумовлює різний зміст ознак об'єктивної сторони комп'ютерних злочинів, пов'язаних зі знищенням інформації, та умисного знищення або пошкодження майна. Знищення або пошкодження майна полягає в порушенні, як правило, його фізичної цілісності, а знищення або перекручення комп'ютерної інформації не завжди супроводжується порушенням цілісності її носія. Однак, якщо дії особи – це порушення фізичної цілісності комп'ютерної техніки (ознака об'єктивної сторони злочину проти власності), але мета, яку ставить суб'єкт, полягає в заподіянні шкоди відносинам власності на інформацію, то дії цієї особи слід кваліфікувати як знищення комп'ютерної інформації, оскільки знищення або пошкодження комп'ютерної техніки в цьому випадку є способом вчинення комп'ютерного злочину. Кваліфікувати подібні дії необхідно як сукупність злочинів, передбачених ст. 361 або ст. 362 КК, і, за наявності відповідних ознак, ст. 194 КК (умисне знищення або пошкодження майна).

Визначаючи критерії відмежування комп'ютерних злочинів від інших злочинів проти власності, зазначимо, що досить часто комп'ютерна техніка виступає знаряддям або засобом вчинення злочинів проти власності. Видається можливим виділити два найбільш поширені варіанти кваліфікації таких випадків.

По-перше, комп'ютерна техніка може використовуватися для вчинення розкрадань. Такі злочини неодноразово траплялися в практиці правоохоронних органів України. Так, у 1995 р. 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 в 1994 р. у Черкаській обласній дирекції Укрсоцбанку вчинено викрадення 990 млн крб.[2] Правоохоронні органи України в 1996 р. запобігли спробам незаконного переказу з рахунка Національного банку України в АКБ «Таврія» 10 млн. грн., спробам втручання в електронну систему Мелітопольського відділення АК АПБ «Україна» із метою крадіжки 448 тис. грн., а також спробам крадіжки 182 тис. грн. із використанням електронних міжбанківських розрахунків у Закарпатському відділенні банку «Аваль»[3]. Восени 1998 р. з використанням комп'ютерної системи електронних платежів близько 80 млн грн. було викрадено з рахунків Вінницької дирекції НБУ[4].

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 р. в Луганському відділенні АКБ «Укркомунбанк» бухгалтер операційного відділу використала комп'ютерну систему банку для викрадення 300 тис. грн. 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 великих розмірах. Ознаки комп'ютерного злочину в таких діях відсутні, оскільки винний, віддаючи команду комп'ютерній системі переказу

---

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

[2] Див.: *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] Див.: *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 / Керівн. авт. кол. А. І. Комарова, О. О. Крикун.– К., 1998.– С. 148–154.

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

платежів, не перекручує і не знищує комп'ютерну інформацію, яка зберігається в ній, і не завдає шкоди безпеці використання комп'ютерної техніки. Кримінальний кодекс містить спеціальну норму для кваліфікації таких дій. Частина 3 ст. 190 передбачає кримінальну відповідальність за шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки. Необхідно відзначити, що ця норма викликає багато зауважень у науковців і практиків. Насамперед вони стосуються того, що шахрайство є злочином, пов'язаним з обманом, тобто повідомленням неправдивих відомостей *людині,* або зловживанням *довірою людини,* а отже, «не можна обманути комп'ютер або зловжити його довірою»[1].

Однак при вчиненні такого шахрайства обманюється ніяк не комп'ютер, а людина, яка використовує комп'ютер для інтенсифікації діяльності, наприклад, щодо банківських розрахунків. Має місце, можна сказати, опосередкований обман, тобто певні неправдиві відомості повідомляються не безпосередньо людині, а опосередковано, через комп'ютер. Тому вказана норма «має право на існування», та, ураховуючи, що використання комп'ютерної техніки значно підвищує ступінь суспільної небезпечності шахрайства, її використання видається доцільним.

Як приклад застосування ч. 3 ст. 190 КК розглянемо вирок Корольовського районного суду м. Житомира у справі № 1-81/2007 від 5 січня 2007 р.[2] щодо обвинувачення Ц. та Ч. Серед злочинів, які їм інкримінувалися, були посягання, передбачені ч. 2 ст. 361 та ч. 3, ст. 190 КК України. Так, 26 березня 2006 р. близько 8 год, Ц. за попередньою змовою із Ч., з метою заволодіння чужим майном через обман з використанням електронно-обчислювальної техніки, зайшли до приміщення Пункту колективного користування послугами Інтернет, розташованого у відділенні зв'язку № 7 Житомирської філії відкритого акціонерного товариства «Укртелеком», що по вул. Вітрука, 26 в м. Житомирі. Після чого Ц., діючи спільно із Ч. щодо реалізації свого злочинного наміру, з використанням комп'ютера, підключеного до мережі Інтернет із IP-адресою, за-

[1] *Законодавство* про кримінальну відповідальність за «комп'ютерні» злочини: Науково-практичний коментар і шляхи вдосконалення / А. А. Музика, Д. С. Азаров.– К.: Вид. Паливода А. В., 2005.– С. 56–57.

[2] *Вирок* Корольовського районного суду м. Житомира по справі № 1-81/2007 від 5 січня 2007 р. // Єдиний державний реєстр судових рішень.– Режим доступу: http://www.reyestr.court.gov.ua/

кріпленою за сервером вказаного Пункту колективного користування послугами Інтернет, що обслуговується Житомирською філією ВАТ «Укртелеком», шляхом підбору випадкових цифр логінів, паролей та трансферів, ввели в оману автоматизовану систему і видавши себе за законного користувача, вчинили несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж для доступу до програмного комплексу віддаленого обслуговування клієнтів сайту, належного закритому акціонерному товариству комерційний банк (ЗАТ КБ) «ПриватБанк». Внаслідок несанкціонованого втручання, зазнала витоку та блокуванню конфіденційна інформація про користувачів автоматизованої системи та інформація про банківський рахунок клієнта банку гр-на Т.

Отримавши доступ до конфіденційного рахунка по кредитній картці клієнта банку Т., Ц. за попередньою змовою із Ч., продовжуючи свої злочинні дії, за рахунок кредитних коштів ЗАТ КБ «ПриватБанк», в період з 10 год 08 хв до 10 год 43 хв через мережу Інтернет вчинили 6 фінансових операцій по придбанню 6 електронних ваучерів Закритого акціонерного товариства (ЗАТ) «Київстар GSM» на поповнення рахунка мобільного телефону на загальну суму 1525 грн. Отримавши з автоматизованої системи текстове повідомлення про авторизацію проведених операцій з зазначенням ідентифікаційного коду придбаних ваучерів, Ц. та Ч., в період з 11 год 22 хв до 11 год 26 хв через введення кода ваучерів у свій мобільний телефон «BOSCH», із абонентською скретч-карткою «Київстар GSM» для мобільного зв'язку, вчинили фінансову операцію та поповнили рахунок своєї скретч-картки на загальну суму 1525 грн. тобто заволоділи чужим майном способом обману.

Також у вироку зазначається, що в період з 26 березня по 13 квітня 2006 р. подібні дії (несанкціоноване втручання та подальше шахрайство) Ц. та Ч. вчинили ще відносно 10 потерпілих. У зв'язку з чим суд під час кваліфікації означених діянь врахував ознаку повторності.

Крім цього суд зазначив, що вважає за необхідне кваліфікувати дії обох підсудних за сукупністю злочинів, передбачених *ч. 2 ст. 361, ч. 3 ст. 190 КК України*, оскільки підсудні, використовуючи комп'ютерну техніку *незаконно, без відповідного санкціонування, втрутились у діяльність комп'ютерної мережі* (сервера «Приват 24») та *отримали відповідну інформацію щодо кількості грошей на рахунках клієнтів банку, викрадали з них тільки частину коштів, що знаходились на їх рахунках – тобто умисно створили умови*

для витоку відповідної інформації щодо кількості грошей на відповідних рахунках, логінів та паролів входу до відповідної комп'ютерної інформації, через застосування нових паролів *блокували* відповідні платіжні картки, після чого *шахрайськими діями заволоділи чужим майном – грішми*, які знаходились на картках клієнтів ЗАТ КБ «ПриватБанк»; при цьому в контексті диспозиції ст. 361 ч. 2 КК України «витік інформації» не слід розуміти, як її поширення невизначеній кількості отримувачів даної інформації. Таким чином, Кримінальний Закон не дозволяє кваліфікувати дії обох підсудних лише за ст. 190 ч. 3 КК України, оскільки їх дії щодо несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж, що призвело до витоку, блокування, підробки інформації не можуть рахуватись лише як спосіб шахрайського заволодіння чужим майном з використанням комп'ютерної техніки.

Слід зазначити, що на сьогодні ще одним з видів шахрайства, вчинюваного з використанням електронно-обчислювальної техніки, є так званий фішинг. Він полягає в тому, що зловмисники масово надсилають електронні листи, у яких від імені якогось відомого банку, Інтернет-магазину, фінансової компанії чи під іншим приводом, наприклад виграш у лотереї, пропонують адресатам повідомити реквізити своєї пластикової картки, а потім використовують ці реквізити для заволодіння грошима адресатів.

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*. Найпоширенішим видом подібних посягань у вітчизняній практиці є отримання доступу до мережі Інтернет за рахунок законних абонентів через використання їх логінів та паролів. Видається, що правильною кваліфікацією подібних дій, у контексті злочинів проти власності, є їх оцінка за ст. 192 КК України. Однак, відповідальність за даною нормою настає лише у випадку заподіяння матеріальної шкоди, що перевищує 50 неоподатковуваних мінімумів доходів громадян. Оскільки шкода, що заподіюється внаслідок більшості крадіжок машинного часу, значно менша, подібні дії отримують правову оцінку як блокування комп'ютерної інформації законних користувачів тим часом, коли за їх рахунок та під їхніми іменами порушники отримували доступ до інформації (ст. 361),

а також, якщо отримання чужих логінів і паролів здійснювалося у спосіб несанкціонованого втручання або особою, яка має доступ до комп'ютерної інформації, відповідно як несанкціоноване втручання, що призвело до витоку комп'ютерної інформації (ст. 361), або як злочин, передбачений ст. 362 КК.

Так, у вироку Голованівського районного суду Кіровоградської області по справі № 1-156/08 від 16 вересня 2008 р.[1] щодо обвинувачення Р. у вчиненні злочину, передбаченого ч. 1 ст. 361 КК України, зазначається таке. 2 квітня 2001 р. Голованівське відділення Гайворонської міжрайонної державної податкової інспекції (надалі МДПІ) уклало договір № 26 з Голованівським ЦЕЗ № 7 Кіровоградської філії ВАТ «Укртелеком» про надання доступу до мережі Інтернет.

20 вересня 2007 р. п. 1.3 наказу № 79 Гайворонської МДПІ призначено адміністратором мережі Інтернет Голованівського відділення Гайворонської МДПІ головного державного податкового інспектора відділу інформатизації процесів оподаткування Р-ву.

У січні 2008 р. Р., перебуваючи в Голованівському відділенні Гайворонської МДПІ в кабінеті своєї дружини Р-вої під час здійснення уповноваженою особою Р-вою процедури під'єднання до мережі Інтернет, діючи умисно, незаконно дізнався про інформацію з обмеженим доступом – логін та пароль доступу до мережі Інтернет вказаного відділення Гайворонської МДПІ.

Після цього, в період з 28 січня по 11 червня 2008 р. Р., діючи умисно, без дозволу керівництва Голованівського відділення Гайворонської МДПІ, незаконно використовуючи логін та пароль доступу до мережі Інтернет Голованівського відділення Гайворонської МДПІ з власного комп'ютера (Pentium 4,3 GHz RAM 512 MB ОЗУ) з умонтованим внутрішнім модемом ACORP M56PML-G та накопичувачем на твердих магнітних дисках (HDD) № WCAM9A318646 Western Digital 800, підключеного за допомогою мережевого кабелю до роз'єму телефонної мережі, призначеного для підключення телефонного апарату з номером, що зареєстрований за Р., неодноразово здійснював несанкціоноване втручання в роботу комп'ютерної мережі Інтернет, що призвело до блокування інформації Голованівського відділення Гайворонської МДПІ щодо звітності платників податків.

[1] Вирок Голованівського районного суду Кіровоградської області по справі № 1-156/08 від 16 вересня 2008 року // Єдиний державний реєстр судових рішень.– Режим доступу: http://www.reyestr.court.gov.ua/

Згідно висновку експерта з магнітного носія № WCAM9A318646 Western Digital 800, що міститься в системному блоці (Pentium 4,3GHz RAM 512 MB ОЗУ) здійснювалось підключення до мережі «Інтернет» за допомогою комутованого зв'язку, виклики відбувались з використанням логіну Голованівського відділення Гайворонської МДПІ. Логін та пароль користувача жорстко пов'язані між собою, тобто з допомогою вищевказаного логіну користувач не може підключитися до Інтернету з використанням будь-яких інших паролів. Одночасна робота двох користувачів з однаковими логіками та паролями не можлива. Таким чином, *при виході в Інтернет будь-якої сторонньої особи доступ власнику логіну блокується.*

Коментуючи цей вирок, зазначимо також, що Р. було здійснено більше 15 підключень з використанням вказаних логіну та пароля, однак суд дав їм правильну оцінку як одиничному, продовжуваному злочину, оскільки всі ці факти несанкціонованого втручання охоплювалися єдиним умислом та, відповідно, не утворювали повторності злочинів.

По-друге, «комп'ютерний» злочин може бути способом вчинення злочину проти власності. У цих випадках дії необхідно кваліфікувати за двома статтями: статтею, що передбачає відповідальність за злочин проти власності, і статтею, що передбачає відповідальність за «комп'ютерний» злочин. Як приклад можна навести такий випадок. З вересня до грудня 1999 року в Донецьку (досудове слідство провадилося прокуратурою Донецької області) головний інженер-програміст Центру інформаційних технологій і технічного забезпечення Донецької дирекції Українського державного підприємства електрозв'язку «Укртелеком» розробив комп'ютерну програму, яка дає змогу відшукувати в масиві фіксованої структури телефонні розмови, проведені з заданих номерів телефонів, відбирати їх і 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. Унаслідок таких дій підприємству електрозв'язку було заподіяно збитки у розмірі близько 150 тис. гривень. Кваліфікувати дії головного інженера, якби вони були вчинені після набрання чинності змін до КК України, що передбачили нову редакцію розділу XVI КК, необхідно було б за сукупністю злочинів, передбачених ст. 192 КК (спричинення значної матеріальної шкоди через обман без ознак шахрайства), ст. 361 КК (несанкціоноване втручання в роботу автоматизованої системи обчислення плати за надання послуг міжміського та міжнародного зв'язку, яке спричинило підроблення комп'ютерної інформації) та ст. 361-1 КК (створення з метою використання шкідливої програми, призначеної для несанкціонованого втручання в роботу автоматизованої системи).

Схожий випадок стався влітку 2002 р. в Херсоні. Студент одного з вузів міста вчинив несанкціоноване 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 11 000 грн.[1] За чинним КК подібні дії необхідно кваліфікувати як сукупність злочинів, передбачених статтями 192 і 361 КК.

2. На окрему увагу заслуговує питання відмежування комп'ютерних злочинів від злочинів, що полягають у збиранні інформації з обмеженим доступом (статті 111, 114, 231 та 330 КК України). Ці злочини, якщо їх предметом є відомості, що становлять певну таємницю та є комп'ютерною інформацією, збігаються за ознаками об'єктивної сторони з несанкціонованим втручанням, що призвело до витоку інформації (ст. 361) або несанкціонованим перехопленням чи копіюванням, якщо воно призвело до витоку інформації (ч. 2 ст. 362). Однак обов'язковою ознакою суб'єктивної сторони зазначених некомп'ютерних злочинів є мета – використання інформації, що є предметом посягання. У разі відсутності такої мети вчинене, за наявності відповідних ознак, необхідно кваліфікувати як злочин, передбачений ст. 361 або ст. 362 КК України. Слід зазначити, що в практиці зарубіжних правоохоронних органів траплялися випадки посягання на закриту комп'ютерну інформацію без мети її використання. Наприклад, у лютому 1998 р. громадянин Ізраїлю Еуд 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 дають можливість кваліфікувати його

[1] Див.: *Свиридов С.* «Капкан» для хакера // Комсомольская правда.– 2002.– 10 сентября.– С. 5.

дії як шпигунство[1]. Як би ці події відбувалися на території України, то дії ізраїльського громадянина треба було б кваліфікувати як несанкціоноване втручання в роботу електронно-обчислювальних машин, яке призвело до витоку комп'ютерної інформації (ст. 361 КК).

3. Досить важливою проблемою є також відмежування злочинів, пов'язаних з розголошенням або передаванням відомостей з обмеженим доступом (статті 111, 114, 132, 145, 168, 182, 232, 328, 330, 381, 387, 422), від несанкціонованого збуту або поширення комп'ютерної інформації з обмеженим доступом (ст. 361-2 КК). Розмежування в даних випадках, головним чином залежить від ознак складу злочину, що характеризують *суб'єкта* або *особу, якій передаються відомості*.

Так, відмежування злочинів, передбачених статтями 111, 114 та 330 КК (якщо відомості, що становлять їх предмет, є комп'ютерною інформацією), від несанкціонованого збуту або розповсюдження комп'ютерної інформації з обмеженим доступом (ст. 361-2 КК) слід проводити на підставі аналізу *ознак, що характеризують особу, якій передається комп'ютерна інформація.* Наприклад, якщо комп'ютерна інформація, що становить державну таємницю, передається представникові іноземної організації, наявним є склад злочину, передбачений ст. 111 або ст. 114 КК. Однак, якщо така інформація передається іншій особі, дії (за відсутності ознак складу злочину, передбаченого ст. 328 КК) необхідно кваліфікувати за ст. 361-2 КК.

Злочини, передбачені статтями 132, 145, 232, 328, 330, 381, 387 та 422 КК (якщо їх предметом є відповідна комп'ютерна інформація), необхідно відмежовувати від несанкціонованого збуту або поширення комп'ютерної інформації (ст. 361-2 КК) за ознаками суб'єкта. Усі перелічені некомп'ютерні злочини характеризуються наявністю спеціального суб'єкта, тому поширення або збут комп'ютерної інформації, що є предметом цих злочинів, загальним суб'єктом необхідно кваліфікувати за ст. 361-2 КК. Крім того, обов'язковою ознакою об'єктивної сторони незаконного розголошення лікарської таємниці (ст. 145 КК) є настання тяжких наслідків, а розголошення комерційної або банківської таємниці (ст. 232) – істотної шкоди, тому поширення комп'ютерної інформації, яка

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

містить лікарську, банківську або комерційну таємниці, що не призвело до названих наслідків, слід кваліфікувати за ст. 361-2 КК.

Відмежування складу злочину, передбаченого ст. 361-2 КК, від розголошення таємниці усиновлення (удочеріння) (ст. 168 КК) та поширення конфіденційної інформації про особу (ст. 182 КК) здійснюється передовсім на підставі ознак об'єкта та суб'єктивної сторони. Несанкціоновані поширення або збут комп'ютерної інформації відносять до злочинів проти власності на неї, тим часом як розголошення таємниці усиновлення та поширення конфіденційної інформації про особу відносять до злочинів проти відповідних конституційних прав людини і громадянина. Отже, якщо особа усвідомлює, що вона, наприклад, поширює конфіденційну інформацію про конкретну особу або конкретну, персонально визначену групу осіб без їх згоди, має місце злочин проти конституційних прав та свобод – порушення недоторканності приватного життя (ст. 182). Але, якщо особа не усвідомлює, чиї саме персональні дані вона поширює, наприклад, розміщує на Інтернет-сайті електронну базу паспортних даних осіб, що прописані у певному місці, яка належить міському відділу внутрішніх справ, має місце злочин проти права власності на комп'ютерну інформацію з обмеженим доступом (у такому разі проти державної власності на комп'ютерну інформацію), тобто злочин, передбачений ст. 361-2 КК України.

4. Несанкціоновані дії, що призвели до витоку комп'ютерної інформації (ст. 361 та ч. 2 ст. 362 КК), 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 належить до комп'ютерних злочинів, а є злочином проти особистих прав і 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, а саме кореспонденція; а також за об'єктом посягання: право власності на комп'ютерну інформацію та недоторканність приватного життя. Зазначимо, що мова йде лише про приватну кореспонденцію, тобто про листування між фізичними особами або між фізичною та юридичною особою. Ознайомлення зі змістом листування між юридичними особами слід кваліфікувати, за наявності мети розголошення або іншого

використання отриманих відомостей, як умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю (ст. 231), або, у разі відсутності такої мети й залежно від ознак суб'єкта, як злочин, передбачений ст. 361 або ст. 362 КК.

Значний інтерес, в контексті питання відмежування комп'ютерних злочинів від порушення таємниці кореспонденції, представляє собою вирок Першотравневого районного суду м. Чернівці по справі № 1-235/2008 від 29 серпня 2008 р.[1] щодо обвинувачення Д. у вчиненні злочинів, передбачених ч. 2 ст. 361-1, ч. 2 ст. 361 та ч. 1 ст. 163 КК України. Так, Л., використовуючи власний комп'ютер для комутованого доступу до мережі Інтернет, зіткнувся з проблемою захисту комп'ютера від шкідливих комп'ютерних програм (комп'ютерних вірусів). Оскільки в мережі Інтернет цих шкідливих програм дуже багато, то таке явище, як порушення роботи комп'ютера, внаслідок дії цих програм дуже актуальне для кожного користувача. Зацікавившись темою вірусів, він дізнався, що є категорія вірусів, які можливо створити способом спеціального налаштування вже створених програм. Однією з таких програм є Ardamax keyloger 2.9. Ця програма є трояном кейлогером, яка здійснює електронне шпигунство за користувачем зараженого комп'ютера: інформація, що вводиться з клавіатури, знімки екрана і дії користувача зберігаються у файлі на диску і періодично відправляються зловмисникові. В мережі Інтернет він відшукав дистрибутив цієї програми і скачав собі в комп'ютер. Ознайомившись детально з принципом її дії, він налаштував цю програму таким чином, щоб всю інформацію, яку вона збирала в чужих комп'ютерах, відправляла на його електронну скриньку. Його власне налаштування програми Ardamax keyloger 2.9 фактично перетворило її в троянську програму «Trojan-Spy.Win32.Ardamax.n». Усвідомлюючи, що створена ним комп'ютерна програма є шкідливою програмою, призначеною для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), Л. вирішив поширити її серед необмеженої кількості користувачів локальної мережі «Вегателеком». Так, за допомогою власного комп'ютера і стандартного програмного забезпечення операційної системи Microsoft Windows XP SP2 для доступу в Інтернет, Л. 9 квітня 2008 р. о 10 год навмисно розмістив шкідливу комп'ютерну програму

[1] *Вирок* Першотравневого районного суду м. Чернівці по справі № 1-235/2008 від 29 серпня 2008 р. // Єдиний державний реєстр судових рішень.– Режим доступу: http://www.reyestr.court.gov.ua/

«Trojan-Spy.Win32.Ardamax.n» під назвою Winamp_6.0_New Edition.exe на сервері локальної комп'ютерної мережі «Вегателеком». Знаючи, що Winamp.exe – це назва популярного програвача комп'ютерної музики та фільмів, він тим самим намагався приховати від користувачів справжнє призначення цієї шкідливої програми і таким чином змусити активізувати її. Залишаючись доступними для необмеженої кількості користувачів локальної мережі компанії «Вегателеком», Л. створив всі необхідні умови для його поширення. Знаходячись на сервері, шкідливий програмний засіб «Trojan-Spy.Win32.Ardamax.n» став доступний для Ю., яка 9 квітня 2008 р. активізувала його, вважаючи за легальну комп'ютерну програму. Після зараження комп'ютера Ю., троянська програма «Trojan-Spy.Win32.Ardamax.n» стала в автоматичному режимі вести електронний журнал натискання користувача на клавіатуру, та робити знімки з робочого столу (монітора), після чого зібрану інформацію в період з 9 квітня до 16 травня 2008 р. періодично відправляла в електронну скриньку Л. В результаті йому стали відомі реквізити авторизації Ю. без її згоди: логін та пароль, назва її електронної скриньки та пароль до неї, а також зміст її розмов з друзями та знайомими, здійснені за допомогою комп'ютерної програми jajc.exe (програми обміну миттєвих текстових повідомлень), що становлять її особисту таємницю.

У результаті своїх злочинних дій Л., *створив та розповсюдив шкідливий програмний засіб* і *несанкціоновано втрутився в роботу електронно-обчислювальної машини* (комп'ютера) Ю., *що призвело до витоку інформації*, а також *порушив таємницю кореспонденції*, що передається через комп'ютер.

У цьому випадку суд правильно оцінив той факт, що серед відомостей, отриманих внаслідок несанкціонованого втручання в роботу комп'ютера Ю., є такі, які становлять таємницю кореспонденції, що передається через комп'ютер, а отже вчинене потребує додаткової кваліфікації за ст. 163 КК. Крім цього, звернімо увагу ще й на те, що Л., як вказано у вироку (для прикладу ми навели лише частину цього документа), здійснив подібні дії, тобто розповсюдження троянської програми та несанкціоноване отримання внаслідок її роботи на комп'ютерах потерпілих відповідних відомостей, стосовно ще шести потерпілих. Таким чином, Л. фактично здійснив кілька розповсюджень шкідливих програм, несанкціонованих втручань та порушень таємниці кореспонденції. Суд, застосовуючи правила кваліфікації при повторності злочинів, надав вчиненим діянням правильну правову оцінку – як злочинам, вчиненим повторно.

5. Важливим питанням у визначенні критеріїв відмежування комп'ютерних злочинів від суміжних є формулювання ознак, які дають можливість розмежувати несанкціоноване втручання, що спричинило втрату або підробку комп'ютерної інформації (ст. 361 КК), або несанкціоновану зміну чи знищення комп'ютерної інформації, вчинену особою, яка мала право доступу до неї (ст. 362 КК), і злочини, передбачені ст. 357 КК «Викрадення, присвоєння, вимагання документів, штампів, печаток, заволодіння ними шляхом шахрайства чи зловживання службовим становищем або їх пошкодження», ст. 358 КК «Підроблення документів, печаток, штампів та бланків, їх збут, використання підроблених документів» та ст. 366 КК «Службове підроблення». Оскільки документ є одним із видів інформації, подібність зазначених складів полягає в тому, що статті 357, 358, 366 та статті 361 і 362 КК України передбачають відповідальність за знищення або перекручення інформації. Видається можливим сформулювати таке правило: у тих випадках коли документ, що є предметом злочинів, передбачених статтями 357, 358 або 366, є комп'ютерною інформацією, електронним, дії особи щодо його підроблення або знищення потребують, залежно від ознак суб'єкта, додаткової кваліфікації за ст. 361 або ст. 362 КК України. Таке правило пояснюється тим, що в означених випадках спосіб підробки або знищення документа становить самостійний склад злочину. У цьому випадку передусім йдеться про електронні документи, до яких відповідно до Закону України «Про електронні документи та електронний документообіг» від 22 травня 2003 р. відносяться документи, інформація в яких зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа (ст. 5 Закону).

6. Комп'ютерна технологія привела до появи нових об'єктів інтелектуальної власності: програмного забезпечення та топографій інтегральних мікросхем, які стали новими видами предметів злочинів проти інтелектуальної власності (статті 176, 177 КК України). Отже, необхідним є відмежування несанкціонованого розповсюдження або збуту комп'ютерної інформації з обмеженим доступом (ст. 361-2) від цих злочинів. Різниця таких злочинів полягає в ознаках об'єкта і предмета. Безпосередніми об'єктами злочину, передбаченого ст. 176 КК, є авторські права (особисті немайнові та майнові права авторів, їх правонаступників, пов'язані зі створенням і 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) становлять відносини володіння, розпоряджання, користування результатом *своєї творчості* в будь-якій сфері промисловості чи господарської діяльності[1]. Ці норми *охороняють інтереси автора*, особи, яка створила певні об'єкти інтелектуальної власності. У свою чергу, незаконні розповсюдження або збут комп'ютерної інформації (ст. 361-2 КК) посягають на інший об'єкт – відносини володіння, користування та розпоряджання комп'ютерною інформацією з обмеженим доступом як її авторів, так і осіб, котрі такими не є.

З цього положення випливає другий критерій, який дозволяє відмежувати згаданий комп'ютерний злочин від порушення авторського права, а саме предмет посягання. Предметом першого з названих злочинів є комп'ютерна інформація з обмеженим доступом, предметом останнього – тільки об'єкти авторського права, до яких чинне законодавство України відносить, зокрема, програми для ЕОМ і бази даних.

Слід також зазначити, що потерпілим від злочину, передбаченого ст. 361-2 КК, 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.

Отже, якщо особа розповсюджує за допомогою комп'ютерної мережі, наприклад, електронний варіант популярного художнього твору без згоди автора, наявним є склад злочину, передбачений ст. 176 КК (за умови настання вказаних у статті наслідків). Склад злочину, передбачений ст. 361-2 КК, у даній ситуації відсутній через відсутність предмета: електронний варіант художнього твору не є комп'ютерною інформацією з обмеженим доступом. А якщо предметом розповсюдження буде комп'ютерна інформація з обмеженим доступом, яка одночасно є й об'єктом авторського права, наприклад, електронний варіант підручника з грифом «таємно», матиме місце сукупність злочинів, передбачених статтями 176 та 361-2 КК України.

---

[1] Див.: *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.– К.-Х.: Юрінком Інтер – Право, 2001.– С. 104–107.

7. Необхідно також зазначити, що деякі способи вчинення комп'ютерних злочинів потребують додаткової кваліфікації. Так, використання для несанкціонованого втручання (ст. 361 КК) або несанкціонованого перехоплення чи копіювання (ст. 362 КК) спеціальних технічних засобів негласного отримання інформації потребує додаткової кваліфікації за ст. 359 КК «Незаконне використання спеціальних технічних засобів негласного отримання інформації». Якщо ж несанкціоноване втручання в роботу комп'ютерної мережі або мережі електрозв'язку вчиняється шляхом умисного пошкодження кабельної, радіорелейної, повітряної лінії зв'язку, проводового мовлення або споруд чи обладнання, які входять до їх складу, і це, крім наслідків, передбачених у ст. 361 КК, призводить до тимчасового припинення зв'язку, вчинене належить кваліфікувати за сукупністю злочинів, передбачених статтями 360 та 361 КК України «Умисне пошкодження ліній зв'язку».

Таким чином, комп'ютерна техніка може використовуватися для вчинення багатьох злочинів, однак *використання комп'ютерної техніки ще не дає можливість говорити про те, що скоєно комп'ютерний злочин*. Основним критерієм відмежування цих злочинів від суміжних, пов'язаних із використанням комп'ютерної техніки як знаряддя або засобу, *є об'єкт посягання*.

Запитання для самоконтролю та самоперевірки

1. В яких випадках порушення правил експлуатації ЕОМ слід кваліфікувати за ст. 363 КК України, а в яких – за ст. 362 КК України?
2. Як кваліфікувати масове розповсюдження повідомлень електрозв'язку, яке спричинило блокування комп'ютерної інформації?
3. Наведіть приклади й охарактеризуйте правила кваліфікації випадків, коли комп'ютерна техніка є знаряддям вчинення злочину.
4. Що таке «крадіжка машинного часу»? Як кваліфікувати такі дії?
5. Наведіть приклади й охарактеризуйте правила кваліфікації випадків, коли комп'ютерний злочин є способом вчинення злочину проти власності.
6. Як слід відмежовувати комп'ютерні злочини від злочинів, пов'язаних зі збиранням і розповсюдженням інформації з обмеженим доступом?
7. В яких випадках несанкціоноване втручання, що призвело до підроблення інформації, слід кваліфікувати за ст. 358 КК?

Розділ 9. Напрями вдосконалення кримінального законодавства України про комп'ютерні злочини

Дослідження ознак складів злочинів, передбачених у розділі XVI КК України, дає можливість стверджувати, що інформаційні суспільні відносини на достатньо високому рівні захищені від посягань у сфері використання комп'ютерної техніки. Однак, оскільки розширення сфери застосування ЕОМ та значні досягнення технології зумовлюють постійне зростання комп'ютерної злочинності, ускладнення способів вчинення комп'ютерних злочинів та появу нових видів посягань на інформаційні відносини, то необхідним видається вдосконалення чинного кримінального законодавства. Проведений аналіз ознак складів злочинів, передбачених статтями 361–363-1 КК України, дозволяє сформулювати низку пропозицій щодо вдосконалення кримінального законодавства.

1. Аналіз об'єктивних ознак несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку свідчить про те, що *законодавець передбачив кримінальну відповідальність за абсолютно самостійні склади злочинів в одній нормі*. Несанкціоноване втручання в роботу комп'ютерної техніки та несанкціоноване втручання в роботу мереж електрозв'язку не збігаються, як зазначалось раніше, за ознаками об'єкта, предмета й об'єктивної сторони. У зв'язку із цим видається доцільним передбачити кримінальну відповідальність за несанкціоноване втручання в роботу мереж електрозв'язку в окремій статті КК.

2. Використання в тексті закону таких термінів, як «електронно-обчислювальна машина», «автоматизована система» та «комп'ютерна мережа», видається не зовсім вдалим законодавчим рішенням.

По-перше, це пов'язано з недосконалістю національного законодавства з питань автоматизованого опрацювання інформації, відсутністю єдиного нормативного акта, який містив би чіткі визначення. Так, терміни «електронно-обчислювальна машина» та «комп'ютерна мережа» визначаються державним стандартом (ДСТУ 2938-94. Системи оброблення інформації. Основні поло-

ження. Терміни та визначення. Від 01.01.96), термін «автоматизована система» визначається як у Законі «Про захист інформації в інформаційно-телекомунікаційних системах», так і в державному стандарті (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. Від 01.07.94). Крім того, визначення, наведені в законі та стандарті, принципово різні.

По-друге, доцільність виокремлення в кримінальному законодавстві видів засобів опрацювання комп'ютерної інформації викликає певні сумніви. Від виду такого засобу навряд чи залежить суспільна небезпечність комп'ютерного злочину. Не можна сказати, що несанкціоноване втручання в роботу ЕОМ, наприклад, більш суспільно небезпечне, ніж несанкціоноване втручання в роботу комп'ютерної мережі. Як уже зазначалося, суспільна небезпечність комп'ютерного злочину насамперед залежить від соціальної значущості суспільних відносин власності на інформацію, яким заподіюється шкода, змісту комп'ютерної інформації, що знищується, копіюється, перекручується або блокується.

Нарешті, по-третє, наявність у кримінальному законі переліку засобів оброблення інформації зумовлює певні обмеження його застосування для протидії комп'ютерним злочинам: з появою нових, не передбачених у законі засобів, таке законодавство неможливо буде застосовувати для захисту інформаційних суспільних відносин, пов'язаних із використанням цих засобів.

Тому пропонується не визначати в тексті закону види засобів оброблення комп'ютерної інформації, а використовувати один загальний термін – «комп'ютерна система». Він визначається в Конвенції про кіберзлочинність, прийнятій у рамках Ради Європи 23 листопада 2001 р. та ратифікованій Україною 7 вересня 2005 р. Під *комп'ютерною системою* в Конвенції пропонується розуміти будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більше з яких, відповідно до певної програми, виконує автоматичне опрацювання даних. Такий термін є більш вдалим, оскільки він повністю охоплює ЕОМ, автоматизовану систему і комп'ютерну мережу. Його використання дозволило б зробити редакцію статті більш лаконічною, не «прив'язувати» кримінальне законодавство до певного стану розвитку інформаційних технологій, зробити його у зв'язку із цим більш стабільним.

3. Інформація відповідно до нового законодавства є предметом злочинів, передбачених статтями 361, 361-2 та 362 КК України, однак у кожній з цих статей використовується специфічний тер-

мін. Так, предметом несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361) є інформація; предметом злочину, передбаченого ст. 361-2,– інформація з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створена та захищена відповідно до чинного законодавства; інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, є предметом злочину, передбаченого ст. 362 КК України.

Передусім необхідно відзначити, що використання терміна «інформація, яка оброблюється (або зберігається) в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації» є не зовсім вдалим, оскільки він громіздкий, а за змістом повністю відповідає більш точному термінові «комп'ютерна інформація», що використовувався в попередній редакції розділу XVI КК України. І, як уже зазначалося, навряд чи можна визнати доцільним розмежування термінів «інформація, що оброблюється...» (ст. 362 КК) та «інформація, що зберігається...» (ст. 361-2 КК), оскільки оброблення інформації в ЕОМ, системі чи комп'ютерній мережі обов'язково передбачає її зберігання, а зберігання передбачає оброблення.

Крім того, використання в ст. 361 КК терміна «інформація», найбільш загального, такого, що охоплює всі види інформації, свідчить про намагання законодавця за допомогою одного терміна визначити два принципово різні види інформації, які, судячи з аналізу диспозиції статті, є предметами несанкціонованого втручання: комп'ютерну інформацію та інформацію, що передається мережами електрозв'язку. Як видається, ця ситуація є ще одним наслідком намагання законодавця передбачити кримінальну відповідальність за посягання на різні основні об'єкти в одній нормі й ще раз свідчить про доцільність виділення несанкціонованого втручання в роботу мереж електрозв'язку в окремий склад злочину.

Недоліком чинного законодавства є також використання терміна «інформація» для визначення предмета злочину, передбаченого статтями 361 та 362 КК України. Мова йде про таке питання: чи відносяться до комп'ютерної інформації комп'ютерні програми? Необхідно зауважити, що деякі автори відповідають на це питання

позитивно[1], але це не можна визнати правильним. Поняття «інформація» пов'язане з такою категорією, як «код», тобто зі знанням закономірності зміни стану об'єкта, що відображає, залежно від змін об'єкта, що відображається. Питання про те, чи може «знати» ЕОМ, досить складне, тому що такого роду міркування приводять до проблеми штучного інтелекту.

Зрозуміло, що на сучасному етапі розвитку комп'ютерної технології ЕОМ не виконують функції штучного інтелекту, а отже, вести мову про інформацію у формі, яку «розуміє» машина, теж неправильно. Тому заслуговує на увагу позиція В. Тюхтіна, котрий вважає інформацію властивістю суто людської свідомості та спілкування і пов'язує її з наявністю суб'єкта, який пізнає[2]. Виходячи зі змісту статей 361 та 362 КК України, предметом передбачених ними злочинів є інформація, тому, наприклад, несанкціоноване втручання, що призвело до знищення або спотворення програмного забезпечення, або до несанкціонованого знищення програмного забезпечення особою, яка має право доступу до комп'ютерної інформації, кваліфікувати як злочини, передбачені відповідно статтями 361 або 362 КК, буде неправильно. Такі дії можна кваліфікувати як несанкціоноване втручання, що призвело до блокування інформації, спотворення процесу обробки інформації, порушення встановленого порядку її маршрутизації або як пошкодження чи знищення майна.

Цікаво, що один з основних міжнародних нормативних документів у сфері протидії комп'ютерній злочинності – Конвенція про кіберзлочинність – для позначення предмета комп'ютерних злочинів використовує термін «*комп'ютерні дані*», тобто «будь-яке подання фактів, інформації або концепцій у формі, яка є придатною для обробки в комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою». Отже, під комп'ютерними даними розуміються комп'ютерна інформація і комп'ютерні програми. Якщо предметом злочинів, передбачених статтями 361 та 362 КК України, замість інформації визнати комп'ютерні дані, проблемних питань при кваліфікації незаконних діянь щодо програмного забезпечення можна уникнути. За наявності таких змін у законодавстві знищення чи перекручення як інформації, так і програмного забезпечення можна буде кваліфікувати як знищення або перекручення комп'ютерних даних.

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

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

Предметом злочину, передбаченого ст. 361-2 КК України, є інформація з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створена та захищена відповідно до чинного законодавства.

Зазначимо, що використання терміна «інформація» в цій статті є доречним, адже мова йде про комп'ютерну інформацію з обмеженим доступом, згідно зі ст. 30 Закону України «Про інформацію»[1], до неї відноситься таємна і конфіденційна інформація, тобто саме відомості, які сприймаються людиною.

Однак, указівка на те, що предметом цього злочину є комп'ютерна інформація з обмеженим доступом, яка *захищена* відповідно до чинного законодавства, видається зайвою. Відповідно до Закону України «Про захист інформації в автоматизованих системах» від 5 липня 1997 р. така інформація повинна оброблятись із застосуванням «комплексної системи захисту інформації з підтвердженою відповідністю» (ч. 2 ст. 8 Закону).

Отже, предметом злочину є та інформація, що обробляється в такій системі, і якщо проаналізувати диспозицію ст. 361-2 можна дійти висновку, що склад злочину, передбачений цією статтею, буде мати місце лише тоді, коли незаконно розповсюджується або збувається інформація, що обробляється із застосуванням комплексної системи захисту. Водночас проблематичним буде застосування цієї норми для кваліфікації тих випадків, коли особа збуває або розповсюджує інформацію з обмеженим доступом, яку, наприклад, було отримано із захищеної комп'ютерної мережі шляхом подолання системи захисту, тобто на момент розповсюдження інформація з обмеженим доступом уже не захищалася спеціальними технічними засобами.

Зауважимо, що подібні випадки траплялися, вони стосувалися незаконного розповсюдження такого виду комп'ютерної інформації з обмеженим доступом, як електронні бази персональних даних. На-

[1] Див.: *Закон* України «Про інформацію» від 02.11.1992 р. // Закони України.– К., 1996.– Т. 4.– С. 72–88.

приклад, у 2003 р. у продажу з'явилися бази даних російських операторів мобільного зв'язку «Мобільні ТелеСистеми» та «Бі лайн». Крім прізвищ абонентів вони містили паспортні дані, адресу місця проживання, індивідуальний номер платника податків та іншу інформацію. Зазначимо також, що ринок персональних даних – це сегмент комп'ютерної злочинності, який швидко розвивається, деякі фахівці оцінюють його в 3 млрд дол. США на рік[1]. Отже, якщо зазначені недоліки редакції статей 361 та 362 КК України певною мірою ускладнюють їх використання, то недосконалість ст. 361-2 КК практично унеможливлює її застосування для протидії новому виду комп'ютерної злочинності, який швидко розвивається[2]. Тому з метою забезпечення більш надійного кримінально-правового захисту інформаційних відносин бажано було б визначити предметом злочину, передбаченого ст. 361-2 КК України, комп'ютерну інформацію з обмеженим доступом і не вказувати в диспозиції таку ознаку, як наявність засобів захисту такої інформації.

Видається, що при подальшому вдосконаленні кримінального законодавства з питань відповідальності за комп'ютерні злочини більш доцільним було б визнати предметом злочинів, передбачених статтями 361 та 362 КК України, комп'ютерні дані (інформацію та програми), а злочину, передбаченого ст. 361-2,– комп'ютерну інформацію з обмеженим доступом.

4. Певні зауваження викликає конструкція об'єктивної сторони складу злочину, передбаченого ст. 361 КК України. Як уже зазначалося, цей склад злочину є матеріальним, його об'єктивна сторона складається з діяння (несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж

[1] Див.: *Сайтарлы Т.* Право граждан на неприкосновенность частной жизни не имеет достаточного правового обеспечения.– Режим доступа: http://www.crime-research.ru/news/21.01.2005/1772

[2] Необхідно зазначити, що персональні дані певною мірою захищені кримінальним законодавством: ст. 182 КК України передбачає відповідальність за порушення недоторканності приватного життя, однак використання цієї норми для протидії незаконним операціям з електронними базами персональних даних видається не зовсім ефективним. Як уже зазначалося, ця стаття забезпечує фрагментарний захист суспільних відносин від аналізованого посягання, адже безпосереднім об'єктом незаконних дій з електронними базами персональних даних є право власності осіб (юридичних або фізичних), які на законних підставах придбали або створили ці бази, а конституційне право на недоторканність приватного життя виступає, як видається, лише додатковим факультативним об'єктом таких діянь.

електрозв'язку), суспільно небезпечних наслідків (витік, втрата, підробка, блокування інформації, спотворення процесу обробки інформації та порушення порядку її маршрутизації) та причинового зв'язку між діянням і наслідками.

Отже, відповідно до чинного законодавства настання вказаних наслідків не буде визнаватися злочином, якщо їм не передувало несанкціоноване втручання в роботу засобів опрацювання інформації. Наприклад, коли електронно-обчислювальна машина не була ввімкнена, тобто принципово неможливим було втручання в її роботу, на жорсткий диск було здійснено вплив потужним електромагнітним випромінюванням, як наслідок виявилася втрата інформації, що знаходилася на ньому. Використання ст. 361 КК для кваліфікації даного випадку виключається, оскільки не було несанкціонованого втручання в роботу ЕОМ. Зазначимо також, що фізичне знищення або пошкодження носія, який був відокремлений від ЕОМ, автоматизованої системи або комп'ютерної мережі, з метою знищення інформації, яка на ньому знаходиться, знову ж таки з цієї самої причини неможливо кваліфікувати за цією статтею. В останньому випадку можна говорити лише про умисне знищення чужого майна, але використання ст. 194 КК допускається лише тоді, коли в результаті знищення було заподіяно шкоду у великих розмірах. Крім того, така кваліфікація не відповідала б об'єкту посягання: шкоду заподіяно інформаційним відносинам, а діяння кваліфікується як посягання на відносини власності на річ.

Без несанкціонованого втручання в роботу ЕОМ, автоматизованих систем або комп'ютерних мереж можливим є й ознайомлення з інформацією, яка в них обробляється. Наприклад, за допомогою спеціального обладнання можливо, знаходячись на певній відстані від ЕОМ, отримувати відеосигнал, який подається на монітор та ознайомлюватися з інформацією, яка відображається на ньому. Блокувати комп'ютерну інформацію також можливо без несанкціонованого втручання в роботу засобу її оброблення.

Отже, вада конструкції об'єктивної сторони складу несанкціонованого втручання (ст. 361 КК) полягає в тому, що вона не враховує можливість заподіяння вказаних у нормі суспільно небезпечних наслідків без вчинення передбаченого в нормі діяння. Крім того, відсутність несанкціонованого втручання (діяння) не означає, що настання даних наслідків втрачає суспільну небезпечність. Як уже неодноразово відзначалося, головним чинником суспільної небезпечності комп'ютерного злочину є значущість інформації.

У зв'язку з цим пропонується виключити з диспозиції ст. 361 КК України вказівку на діяння, а перелічені в диспозиції наслідки

визначити як «несанкціоновані». Виключення з диспозиції вказівки на діяння вимагає також зміни формулювання таких наслідків, як витік і втрата інформації. Їх необхідно замінити відповідно на ознайомлення та знищення комп'ютерної інформації. Також доречно передбачити в цій статті відповідальність за несанкціоноване копіювання та перехоплення комп'ютерної інформації.

Остання пропозиція потребує певного пояснення. Криміналізація несанкціонованого копіювання та перехоплення комп'ютерної інформації зумовлена тим, що: по-перше, ознайомлення (витік, у чинній редакції) з комп'ютерної інформацією не завжди пов'язане з її копіюванням або перехопленням, тобто можливою є ситуація, коли інформацію скопійовано, її витік не відбувся, а посягання мало значний рівень суспільної небезпечності (наприклад, особа несанкціоновано скопіювала базу даних, що належить державному закладу); по-друге, криміналізація несанкціонованого перехоплення передбачена ратифікованою Україною Конвенцією про кіберзлочинність, а чинне кримінальне законодавство передбачає відповідальність за несанкціоноване перехоплення, тільки якщо його було вчинено спеціальним суб'єктом (ст. 362 КК).

5. Як ми вже зазначали, значна шкода при вчиненні комп'ютерного злочину може виявлятися в заподіянні майнової шкоди (якщо вона в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян) або іншої немайнової шкоди. Водночас однаковими в плані кваліфікації будуть, наприклад, несанкціоноване втручання, що спричинило матеріальні збитки в розмірі двадцяти тисяч гривень, і несанкціоноване втручання, що спричинило збитки в розмірі п'ятисот двадцяти тисяч гривень, або несанкціоноване втручання, що спричинило порушення роботи світлофорів у певному мікрорайоні, та несанкціоноване втручання, що спричинило порушення роботи системи радіаційної безпеки АЕС. Саме тому при дослідженні даного складу постає питання про відбиття *диференціації тяжкості заподіяної шкоди* в конструкції складів комп'ютерних злочинів.

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 йдеться про істотну (значну) шкоду, а в інших – про тяжкі наслідки. При цьому аналіз даних норм дає можливість 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.

Так, у ряді складів законодавець прямо вказує на це в примітках до статей (наприклад, ст. 185 «Крадіжка»). Виходячи з аналізу об'єкта й об'єктивної сторони конкретного складу, можна також 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 Особливої частини КК, більш широке поняття, що охоплює не тільки заподіяння матеріальних збитків. Про це може свідчити те, що в окремих випадках 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 низці 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: заподіяння 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.

Отже, характеристика можливих наслідків комп'ютерних злочинів дає змогу дійти висновку, що доцільним, обґрунтованим і таким, що відповідає специфіці їх об'єкта й об'єктивної сторони, було б доповнення статей розділу XVI КК України відповідними частинами, які передбачали б таку кваліфікуючу ознаку, як настання тяжких наслідків, і примітки до ст. 361 частиною другою, яка установлювала б, що під істотною шкодою, якщо вона полягає в завданні матеріальних збитків, слід розуміти таку шкоду, яка в п'ятсот і більше разів перевищує неоподатковуваний мінімум доходів громадян.

6. 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 в статтях 361, 361-1, 361-2, 362 та 363-1 КК України.

Відомо, що в науці та практиці поняття повторності тлумачилося неоднозначно, тому, безперечно, позитивним є те, що новий КК України дав визначення цього поняття, установивши 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 комп'ютерний злочин, передбачений однією зі згаданих статей, слід вважати вчиненим повторно у випадках, коли особа два або більше разів вчинила злочин, передбачений однією статтею.

Аналізуючи загальне поняття повторності, не можна не сказати, що воно значно обмежує можливість урахування підвищеної суспільної небезпечності комп'ютерного злочину, який вчиняється не після тотожного, а після однорідного злочину. Законодавець у ч. 3 ст. 32 КК України передбачає можливість визнання повторним певного злочину за наявності змішаної повторності, тобто вчинення двох або більше злочинів, передбачених різними статтями КК, якщо таку повторність спеціально передбачено в статтях Особливої частини КК.

Тому доцільним було б доповнення примітки до ст. 361 такого змісту:

«У статтях 361–362 та 363-1 повторним визнається злочин, вчинений особою, що раніше вчинила будь-який із злочинів, передбачених цими статтями цього Кодексу».

Наявність такого доповнення дозволила б більш чітко враховувати під час кваліфікації суспільну небезпечність посягання, визнавати повторними комп'ютерні злочини не тільки в разі їх вчинення після тотожного, але й після однорідного, передбаченого вказаними статтями.

7. Формулювання ознак спеціального суб'єкта злочину, передбаченого ст. 362 КК України (особа, яка має право доступу до комп'ютерної інформації), видається не зовсім вдалим. Цей недолік можна проілюструвати прикладом. Зловмисник перекрутив комп'ютерну інформацію, розташовану на загальнодоступному сайті в мережі Інтернет. Наприклад, в інформаційному повідомленні про науково-практичну конференцію, розміщеному на сайті певного університету, змінив дату проведення заходу. Оскільки інформація на сайті загальнодоступна, ми маємо констатувати, що цей зловмисник змінив комп'ютерну інформацію, до якої мав право доступу, тобто вчинив злочин, передбачений ч. 1 ст. 362 КК. Зазначимо, що так само буде кваліфікуватися й незаконна зміна цієї інформації, вчинена, наприклад, співробітником інформаційного відділу університету, оскільки він також має право доступу

до інформації, що є предметом посягання. Однак суспільна небезпечність посягання, наведеного в останньому прикладі, видається більшою, оскільки співробітник інформаційного відділу наділений певними правами доступу до комп'ютерної інформації не тільки на підставі того, що вона є загальнодоступною, а й у зв'язку з займаною ним посадою. Таким чином, наявне в законі формулювання спеціального суб'єкта злочину, передбаченого ст. 362 КК,– «особа, яка має право доступу до інформації» – не повною мірою забезпечує можливість урахування при кваліфікації підвищеної суспільної небезпечності посягання, вчиненого особою, яка має певні повноваження щодо комп'ютерної інформації, обумовлені її специфічним статусом.

Таке становище, 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. Можна сказати, що в цій ситуації «дух» закону не відповідає його «букві».

Зважаючи на вищесказане, а також на те, що предметом злочину, передбаченого ст. 362 КК, пропонується визнавати комп'ютерні дані, видається доцільним конкретизувати ознаки суб'єкта злочину, передбаченого ст. 362 КК, і визначити його таким чином: *особа, яка має правомірний доступ до комп'ютерних даних у зв'язку з займаною посадою або спеціальними повноваженнями.*

До числа таких осіб слід включати працівників підприємств, установ або організацій, функціональні обов'язки яких передбачають використання комп'ютерних даних, що належать роботодавцеві, для виконання завдань, які стоять перед ними (інженери-програмісти, оператори ЕОМ, адміністратори комп'ютерних мереж тощо). До таких осіб відносяться і працівники правоохоронних органів під час виконання спеціальних оперативно-розшукових заходів, пов'язаних із доступом до комп'ютерної інформації. Важливо відмітити, що ознаки спеціального суб'єкта в такій редакції статті матимуть тільки безпосередні користувачі ЕОМ, систем або комп'ютерних мереж. Допоміжний персонал (водії, охоронці, слюсарі тощо) хоча й може мати певний доступ до ЕОМ, системи або комп'ютерної мережі, проте до спеціальних суб'єктів даного злочину не належить, через те, що не має санкціонованого доступу до інформації.

Не зовсім вдалим є й законодавче визначення суб'єкта злочину, передбаченого ст. 363 КК. Таким суб'єктом є особа, яка відповідає за експлуатацію ЕОМ, автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку. Слід погодитися із зауваженням

Д. С. Азарова про те, що «не може вважатися злочином порушення правил (порядку) захисту інформації, вчинене особою, яка за забезпечення цього захисту відповідає, а за дотримання правил експлуатації техніки – ні»[1]. Можливо, більш правильним було б таке визначення – особа, яка відповідає за дотримання вимог інформаційної безпеки.

8. Одним із актуальних питань протидії суспільно небезпечним посяганням у сфері використання комп'ютерної техніки є питання відповідальності за розповсюдження спаму (SPAM, sending of predatory and abusive e-mail). Термін «спам» визначається в Правилах надання та отримання телекомунікаційних послуг, що затверджені постановою Кабінету Міністрів України № 720 від 9 серпня 2005 р. Під ним розуміються не замовлені попередньо споживачами електронні повідомлення, які або є масовими, або в яких не наведено достовірних відомостей про повну назву, власну поштову чи електронну адресу замовника чи відправника цих повідомлень, або подальше отримання яких споживач не може припинити шляхом інформування про це замовника чи відправника.

Отже, розповсюдження спаму, як правило, полягає в надсиланні великій кількості адресатів повідомлень, які вони не замовляли. Суспільна небезпечність такого діяння має певну специфіку. З точки зору конкретного користувача матеріальні збитки від розповсюдження спаму незначні, вони, врешті-решт, зводяться до оплати Інтернет-послуг, пов'язаних з отриманням зайвої кореспонденції. Однак з точки зору провайдерів, організацій, що надають послуги доступу до Інтернету, спам є досить небезпечним явищем, оскільки його наявність створює зайве, некорисне навантаження обладнання й ускладнює роботу інформаційної системи. Ще одним показником суспільної небезпечності спаму є втрата робочого часу працівників підприємств, установ та організацій, які використовують Інтернет у своїй роботі. Зазначимо, що за даними компанії «Ашманов і Партнери», яка є провідним виробником антиспамерського програмного забезпечення в Росії, обсяг спаму в російському поштовому Інтернет-трафіку у 2004 р. становив 75–80%, а збитки від його розповсюдження – мінімум 250 млн євро[2]. Аналогічні дані

[1] *Законодавство* про кримінальну відповідальність за «комп'ютерні» злочини: Науково-практичний коментар і шляхи вдосконалення / А. А. Музика, Д. С. Азаров.– К.: Вид. Паливода А. В., 2005.– С. 78.

[2] Див.: *Ашманов И., Власова А., Тутубалин А.* Спам 2004: подробный аналитический отчет.– Режим доступа: http://www.cyber-crimes.ru/statistic/Spam-2004_detail.html

про поширення спаму в українському сегменті Інтернет відсутні, але з великою вірогідністю можна прогнозувати, що подібні проблеми очікують українських користувачів мережі Інтернет і провайдерів у найближчому майбутньому. Чи готове українське законодавство до цього?

На жаль, на це питання неможливо відповісти позитивно. Стаття 363-1 КК України передбачає відповідальність за масове розповсюдження повідомлень електрозв'язку, однак кримінальна відповідальність у разі вчинення таких дій настає тільки тоді, коли спричинено наслідки у виді порушення або припинення роботи ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Як уже зазначалося, розповсюдження спаму, як правило, не призводить до таких наслідків. Ситуація, коли в результаті масового розповсюдження повідомлень електрозв'язку настають зазначені наслідки, є винятковою. Порушення або припинення роботи засобів опрацювання інформації слід віднести до абсолютно нетипових наслідків розповсюдження спаму. Тому приклад, який наводився в розділі, присвяченому аналізу складу злочину, передбаченого ст. 363-1 КК, можливо, є єдиною ситуацією, коли ця норма «спрацьовує».

Отже, інформаційні суспільні відносини через недосконалість ст. 363-1 КК України практично не захищені від посягань, пов'язаних із розповсюдженням спаму. «Звичайне» розповсюдження спаму не можна кваліфікувати за даною нормою, оскільки воно не призводить до наслідків, зазначених в ст. 363-1 КК.

Таким чином, ще одним напрямом удосконалення національного кримінального законодавства про комп'ютерні злочини є приведення ст. 363-1 КК у відповідність до специфіки посягань, пов'язаних із поширенням спаму. Для цього, як видається, слід передбачити як наслідки масового розповсюдження не порушення або припинення роботи засобів опрацювання інформації, а значну шкоду.

9. Розвиток сучасних систем телекомунікацій і комп'ютерних мереж привів до такої ситуації, коли протидія комп'ютерним злочинам не може бути достатньо ефективною, якщо вона здійснюється в межах однієї країни[1]. Так званий кіберпростір не має державних кордонів: наприклад, особа, що вчиняє несанкціонований доступ до комп'ютерної інформації, необов'язково має знаходитися

[1] Див.: *Васенин В. А.* Информационная безопасность требует выработки программы на международном уровне.– Режим доступа: http://www.crime-research.ru/news/ 26.10.2004/1560

в тій країні, де фізично розташований носій цієї інформації; автор комп'ютерного вірусу може розмістити його на популярному сайті в мережі Інтернет, що призведе до його поширення в достатньо великій кількості країн. Усе це вимагає узгодження національних кримінальних законодавств і створення єдиного правового простору для забезпечення ефективного захисту від злочинних посягань, пов'язаних із використанням комп'ютерної техніки.

Одним із основних міжнародних нормативних документів у цій сфері є Конвенція про кіберзлочинність, прийнята в рамках Ради Європи 23 листопада 2001 р., з Додатковим протоколом, який стосується криміналізації дій расистського та ксенофобського характеру, вчинених через комп'ютерні системи. У вересні 2005 р. цю конвенцію було ратифіковано Верховною Радою України[1].

Порівняльний аналіз Конвенції та КК України дає можливість констатувати, що більша частина діянь, передбачених нею, визнається злочинами в українському законодавстві. До таких діянь відносяться нелегальне перехоплення (статті 163, 361, 362 КК), втручання в дані (статті 361, 362 КК), втручання в систему (ст. 361 КК), злочини, пов'язані з дитячою порнографією (ст. 301 КК), підробка, пов'язана з комп'ютерами (статті 358, 366 КК), шахрайство, пов'язане з комп'ютерами (ч. 3 ст. 190 КК). Діяння, передбачені Додатковим протоколом до Конвенції, охоплюються ст. 161 КК, яка встановлює відповідальність за порушення рівноправності громадян залежно від їх расової, національної належності або ставлення до релігії, та загальними нормами Особливої частини КК України, що передбачають злочини проти свободи совісті (статті 178–181 КК).

Водночас слід констатувати, що на сьогодні склалася ситуація, коли національне законодавство з питань кримінальної відповідальності за незаконний доступ не відповідає ратифікованій Україною Конвенції.

Незаконний доступ відповідно до Конвенції (ст. 2) вважається закінченим з моменту вчинення діяння, тобто є формальним складом злочину, і полягає у навмисному доступі до цілої комп'ютерної системи або її частини без права на це. В українському ж законодавстві відповідальність за незаконний (несанкціонований[2]) доступ (ст. 361 КК) може наставати лише тоді, коли він призвів до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації; несанкціонований доступ сам по собі, без настання вказаних наслідків, не є злочином. Чи визнавати злочином тільки діяння – несанкціонований доступ, чи є воно настільки суспільно небезпечним? Видається, що ні, а питання про відповідальність за такі дії було б більш доречним у контексті адміністративного права. Проте Конвенцією передбачено можливість криміналізації замість простого несанкціонованого доступу, вчиненого шляхом порушення заходів безпеки. Таке діяння, як видається, уже є достатньо суспільно небезпечним і може бути криміналізоване. Найбільш значущими чинниками його суспільної небезпечності є те, що, по-перше, для подолання заходів інформаційної безпеки, технічного або програмного характеру необхідні спеціальні знання, специфічні навички, що свідчить про підвищену суспільну небезпечність суб'єкта даного злочину, а по-друге, шкода полягає в істотних матеріальних збитках, зумовлених необхідністю відновлення або заміни системи захисту (за даними фахівців з інформаційної безпеки, створення системи безпеки комп'ютерної інформації для великої фінансової установи коштує близько 15 млн дол. США)[1].

Слід зауважити, що в окремих країнах несанкціонований доступ передбачається як самостійний склад злочину[2] (Австралія – ст. 76В частини VI А «Злочини, пов'язані з комп'ютерами» Закону про злочини Зводу законів Співдружності; Німеччина – ст. 202а КК; Італія – ст. 615b КК; Нідерланди – ст. 138а КК; Швейцарія – ст. 143^{bis} КК; Республіка Білорусь – ст. 349 КК). Незважаючи на відмінності в самих визначеннях, у більшості цих норм виділяється ознака, що відбиває не тільки правову специфіку, але й підвищену суспільну небезпечність несанкціонованого доступу. Такою ознакою *є наявність спеціальних засобів захисту комп'ютерної інформації, до якої здійснюється доступ.*

---

[1] Див.: *Закон* України «Про ратифікацію Конвенції про кіберзлочинність» від 7 вересня 2005 р.

[2] Зрозуміло, що терміни «незаконний» і «несанкціонований» не є тотожними. Поняття «несанкціонований доступ» є ширшим за поняття «незаконний доступ», тому повністю охоплює його.

[1] Див.: *Расследование* неправомерного доступа к компьютерной информации / Под ред. Н. Г. Шуруханова.– М.: Щит-М, 1999.– С. 44.

[2] Для аналізу зарубіжного законодавства використано роботу 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

Захист комп'ютерних даних забезпечується різними засобами:
– організаційними;
– технічними;
– програмними.

Організаційні засоби інформаційної безпеки полягають у відповідній роботі з персоналом, який працює з ЕОМ, системами чи комп'ютерними мережами (добір, постійна перевірка, інструктажі), забезпеченні режиму таємності під час функціонування 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: джерела безперервного живлення апаратури, а також пристрої стабілізації напруги, мережні фільтри; засоби екранування апаратури, ліній проводового зв'язку та приміщень, в яких знаходиться комп'ютерна техніка; пристрої визначення та фіксації номера абонента, який отримує доступ до ЕОМ, системи чи комп'ютерної мережі, та інші пристрої, що забезпечують безпеку функціонування комп'ютерної техніки[2].

Програмні засоби захисту комп'ютерної інформації – це комп'ютерні програми, які розроблені та використовуються спеціально для забезпечення безпеки процесів зберігання, передавання й опрацювання комп'ютерної інформації в ЕОМ, системі чи комп'ютерній мережі.

Необхідно також відзначити, що несанкціонований доступ відбувається не тільки тоді, 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 електромережа[3]. Під час роботи ЕОМ створюють наводки в електричній мережі, аналіз яких дає можливість 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.

З урахуванням викладеного вище, несанкціонований доступ можна було б визначити так: *одержання винним можливості ознайомлюватися, знищувати, перекручувати або блокувати комп'ютерні дані, що мають специфічні організаційні, технічні або програмні засоби захисту.*

Таким чином, КК України не повною мірою відповідає Конвенції про боротьбу з кіберзлочинністю, тому необхідно привести національне кримінальне законодавство у відповідність з ратифікованим Україною міжнародно-правовим документом. За умови урахування законодавцем висловлених пропозицій Україна стане повноправною учасницею міжнародної діяльності щодо протидії злочинам у сфері використання комп'ютерної техніки, отримає можливість на якісно новому рівні забезпечувати захист національних інформаційних суспільних відносин.

10. Остання пропозиція не стосується вдосконалення кримінального законодавства, а порушує питання вдосконалення національного законодавства з питань автоматизованої обробки інформації. На сьогодні ефективна протидія комп'ютерній злочинності вимагає не лише наявності відповідного кримінального законодавства, але й чіткої нормативної регуляції інформаційних суспільних відносин. Правове регулювання в цій сфері повинне забезпечити не тільки впорядкування та розвиток цих відносин, але й певною мірою має сприяти попередженню комп'ютерних злочинів. Насамперед це стосується регулювання питань захисту інформації під час її автоматизованої обробки.

Надійний захист інформаційних ресурсів країни – необхідна передумова формування інформаційного суспільства, а отже, й

---

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

[2] Див.: Там само.– С. 40–41.

[3] Див.: *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 р.).– Донецьк: Донецький інститут внутрішніх справ, 2001.– С. 190–199.

обов'язкова умова включення держави до світових процесів інформатизації. Незахищеність інформаційних ресурсів унеможливлює позитивний розвиток країни та призводить до такої ситуації, коли вона позбавляється можливості використовувати новітні технології, стрімко втрачає свої позиції у міжнародному співтоваристві.

Аналіз українського законодавства свідчить, що увага цій важливій проблемі приділяється. Питання інформаційної безпеки регулюються практично на всіх рівнях: прийнято відповідні закони, їх положення конкретизуються указами Президента, рішеннями Кабінету Міністрів, нормативними документами міністерств і відомств. Певний інтерес становить аналіз змісту цих нормативних документів. Основні засади інформатизації встановлюються законами України «Про Концепцію Національної програми інформатизації» та «Про Національну програму інформатизації» від 4 лютого 1998 р. Базовим нормативним документом у сфері захисту комп'ютерної інформації є Закон України «Про захист інформації в автоматизованих системах» від 5 липня 1997 р. У цьому законі формулюється, зокрема, головний принцип регулювання питань захисту комп'ютерної інформації національним законодавством: *відповідальність за захист інформації покладається на власника системи (в якій вона обробляється), при цьому у тих випадках, коли в системі обробляється інформація, що є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, вона повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю*. Тобто, спеціальні вимоги встановлюються лише щодо захисту державної інформації або інформації, захист якої спеціально передбачено в законі. Решта нормативних актів у сфері інформаційної безпеки конкретизує це положення.

Однак статистичні дані свідчать про певну невиправданість такого підходу українського законодавця. Це перш за все дані Українського антивірусного центру: 1) у першому півріччі 2004 р. втрати від вірусних атак в Україні становили 290 млн грн.; 2) найбільші збитки в розрахунку на один ПК спостерігаються в середньому бізнесі, де витрати на технічний захист інформації мінімальні; 3) значно збільшилася кількість вірусних інцидентів, пов'язаних з домашніми користувачами, основна причина масового поширення вірусів у цьому сегменті – практично повна відсутність антивірусних засобів; 4) збитки від вірусних атак в Україні у першій половині 2004 р. зросли на 30% порівняно з аналогічним періодом

2003 р.[1] Отже, можна сміливо стверджувати, що відсутність спеціального нормативного регулювання у сфері захисту недержавної інформації призводить до недостатності заходів щодо захисту такої інформації, які мають здійснюватися її власниками, та, певною мірою, призводить до зростання показників комп'ютерної злочинності.

Таким чином, недостатність заходів захисту недержавного інформаційного ресурсу є одним з віктимологічних факторів комп'ютерної злочинності. Цілком зрозуміло, що ефективним захист інформації буде за умови комплексного використання технічних, програмних та організаційних засобів. Очевидно також і те, що ставити власникам недержавної інформації вимоги, подібні до тих, які передбачаються наведеними нормативними документами, недоцільно, крім того, це навряд чи сприятиме розвиткові відносин інформатизації в країні. Однак проблема законодавчого стимулювання більш широкого використання засобів захисту недержавної інформації все ж існує та потребує якнайшвидшого розв'язання. Отже, ще одним напрямом вдосконалення національного законодавства є створення нормативної бази для розвитку системи захисту недержавної інформації, яка відповідала б можливостям її власників і забезпечувала достатньо надійний захист відповідного сегмента національного інформаційного ресурсу. Це сприятиме запобіганню комп'ютерній злочинності та забезпечить ширші можливості реалізації конституційного права на інформацію.

Викладені в цьому розділі пропозиції знайшли відображення в проекті Закону про внесення змін та доповнень до Кримінального кодексу України (додаток 2).

Запитання для самоконтролю та самоперевірки

1. У чому полягає недосконаліть чинного законодавства, пов'язана з використанням у тексті закону таких термінів, як «електронно-обчислювальна машина», «автоматизована система» та «комп'ютерна мережа»?
2. Що таке комп'ютерна система?
3. Чому використання в тексті закону терміна «комп'ютерні дані» є більш доцільним, ніж використання терміна «комп'ютерна інформація»?

---

[1] Див.: *Украина:* потери от вирусных атак в первом полугодии 2004 г. составили около 45 млн евро.– Режим доступа: http://www.crime-research.ru/news/30.07.2004/1320

4. Наведіть приклади, які демонструють недосконалість конструкції об'єктивної сторони складу злочину, передбаченого ст. 361 КК України?

5. Чому необхідною є криміналізація копіювання та перехоплення комп'ютерної інформації, вчинюваного загальним суб'єктом?

6. Обґрунтуйте необхідність доповнення статей 361–362 та 363-1 КК України такою кваліфікуючою ознакою, як «заподіяння тяжких наслідків».

7. У чому полягає основна проблема використання ст. 363-1 КК України для протидії поширення спаму?

8. Чому необхідною є криміналізація несанкціонованого доступу до комп'ютерної інформації?

Завдання

Завдання 1

Інженера Петренка було звільнено із ЗАТ «Н-ський авіабудівний завод». Бажаючи помститися адміністрації, він прийняв рішення заподіяти шкоду цьому підприємству. Дізнавшись про те, що в квартирі старшого інженера-технолога Кононова знаходиться лазерний диск з програмою управління роботою конвеєра, Петренко проник у квартиру Кононова і вилучив цей диск. Проаналізувавши програму, він розробив власну, яка, будучи запущеною на комп'ютері, за допомогою якого здійснюється управління роботою конвеєра, приводить до його зупинення. Щоб проникнути на завод, Петренко відсканував свій старий пропуск. За допомогою художнього редактора Corel Draw, який він придбав і використовував із порушенням авторського права розробників, змінив дату дійсності пропуску і виготовив його за допомогою кольорового принтера. Пред'явивши цей пропуск на прохідній заводу, Петренко проник на його територію і запустив розроблену ним програму. Збиток від зупинення конвеєра дорівнював 3 млн грн.

Завдання 2

Громадянин Франції М. Бернар розробив комп'ютерну гру «Преферанс» зі спеціальною «закладкою». Цю програму Бернар розташував на своєму сайті в Інтернеті і запропонував вільно копіювати її всім бажаючим. Спеціальна «закладка» в програмі Бернара працювала таким чином: знаходячись в комп'ютері особи, яка скопіювала програму, вона під час чергового сеансу роботи в Інтернеті непомітно для користувача направляла на електронну адресу Бернара ідентифікаційне ім'я (логін) і пароль для підключення до Інтернет, що належать цій особі.

Через місяць після того як Бернар розмістив свою програму в Інтернет, він мав можливість підключатися до міжнародної комп'ютерної мережі від імені і за рахунок більш ніж 150 осіб з Італії, Франції, Іспанії, Польщі, Великобританії та України.

Використовуючи цю можливість, Бернар здійснив несанкціоноване втручання в роботу сервера Міністерства оборони України й отримав доступ до секретної інформації про українське озброєння. Скопіювавши дану інформацію, Бернар не визнав її цікавою і

знищив. У результаті його дій виникла необхідність у зміні системи захисту комп'ютерної інформації Міністерства оборони України, на ці дії було витрачено 150 тис. грн.

Завдання 3

Інженер-програміст обчислювального центру «Кредо-банк» Юрасов розробив програмну «закладку». Така програма в центральному комп'ютері банку відстежувала переміщення сум за рахунками. У разі коли сума, що перераховувалася, перевищувала 20 тис. грн. і на рахунку, з якого вона перераховувалася, знаходилося більше 70 тис. грн., ця програма здійснювала несанкціонований переказ у сумі від трьох до п'яти гривень на спеціальний рахунок. Про «закладку» Юрасов розповів Гриневичу, який працював у тому ж банку і відповідав за відкриття рахунків, і попросив допомогти відкрити рахунок за підробленими документами. Гриневич погодився й оформив відповідні документи за підробленим паспортом, придбаним Юрасовим. Через шість місяців після того як Юрасов помістив «закладку» в центральний комп'ютер банку, на рахунку, відкритому Гриневичем за підробленими документами, було 35 тис. грн.

Завдання 4

Інженера-програміста Петренка було звільнено з ТОВ «Епсилон», де він працював. Бажаючи помститися адміністрації, Петренко в останній день роботи помістив у головний комп'ютер підприємства спеціальну програму. Через п'ять днів після того як Петренко перестав працювати в «Епсилоні», ця програма змінила паролі доступу користувачів корпоративної мережі підприємства. Внаслідок цього жоден зі співробітників протягом трьох днів не мав можливості працювати з діловою інформацією, кореспонденцією, яка надходила, тощо. Збиток від дій Петренка становив 45 тис. грн.

Завдання 5

Директор охоронного агентства «Агата» Васюков, дізнавшись про те, що ВАТ «Українські інформаційні системи» збирається почати діяльність щодо надання населенню доступу до міжнародної комп'ютерної системи Інтернет, запропонував директору цього ВАТ Кульчишину укласти договір про забезпечення інформаційної безпеки його діяльності, мотивуючи тим, що без послуг охоронного агентства діяльність підприємства Кульчишина буде неможливою.

Кульчишин відмовив Васюкову. Після цього Васюков зустрівся з фахівцем з Інтернет-технологій Красненком і розробив з ним операцію щодо заподіяння шкоди ВАТ «Українські інформаційні системи». Згідно з планом Красненко схилив до участі в операції трьох студентів факультету інформатики Кирилова, Завадського і Вознічевського, а Васюков зняв три квартири з телефонами в різних районах міста. У призначений день Васюков закріпив за кожним із залучених студентів по п'ять співробітників агентства для їх охорони й надав кожній групі автомобіль. Групи, установивши устаткування в квартирах, знятих Васюковим, за командою Красненка, почали посилати на сервер ВАТ «Українські інформаційні системи» численні запити на доступ до інформації. Такі дії призвели до відмови сервера ВАТ «Українські інформаційні системи» від обслуговування.

У результаті дій зловмисників близько півтори тисячі клієнтів ВАТ «Українські інформаційні системи» протягом 40 годин були позбавлені можливості працювати з Інтернетом. Дане підприємство надало документи, згідно з якими збиток становив 150 тис. грн. (кошти, необхідні для відновлення роботи сервера, і втрата ділової репутації).

Завдання 6

Лідер однієї з ультраправих організацій Лукін вирішив використовувати комп'ютерну мережу Інтернет для розповсюдження закликів до зміни конституційного ладу України.

Для цього він запропонував інженеру-програмісту Федорову розробити комп'ютерну програму, яка б працювала таким чином: лист, оброблений цією програмою, який направляється електронною поштою, при розкритті його на комп'ютері одержувача автоматично розсилається за адресами всіх абонентів, з якими коли-небудь зв'язувався одержувач. Розробивши таку програму, Федоров передав її Лукіну й одержав від нього 1000 грн.

Після цього Лукін розробив текст листа, що містив заклики до зміни конституційного ладу України, і надіслав його Чернікову. Останній, розкривши його на своєму комп'ютері, автоматично надіслав цей лист Бойченку, Ромащенку і Петренку. Через тиждень після того як Лукін відправив перший лист, його копії одержали 20 000 користувачів Інтернет в Україні.

Завдання 7

Інженер-програміст луганської філії ТОВ «Тандем» Іванов за допомогою спеціальної комп'ютерної програми Quik Link II Fax, яку використовував із порушенням авторського права розробника, здійснював передачу звітної документації в головний офіс ТОВ «Тандем», розташований у Донецьку.

Дізнавшись про це, Москаленко вирішив здійснювати перехоплення цієї кореспонденції. Він розробив спеціальний технічний пристрій, який, будучи приєднаним до телефонного кабелю, що йде з офісу філії ТОВ «Тандем», давав можливість прочитувати інформацію, яку передавав Іванов.

Діючи таким чином, Москаленко ознайомлювався з квартальними звітами філії ТОВ «Тандем» і приватною кореспонденцією Іванова.

Завдання 8

Лисенко, працюючи начальником відділу інформаційної безпеки Донецької обласної дирекції «Укртелеком», розробив комп'ютерну програму, яка надавала змогу відшукувати в базі даних компанії запис, що відповідає конкретному телефонному номеру, і обнуляти в ньому відомості про тривалість здійснених із цього номера міжміських і міжнародних переговорів.

Після цього, вступивши в змову з громадянином Індії, студентом одного з вузів Донецька, Раджівом Махріборті, він надавав послуги міжміського і міжнародного телефонного зв'язку за заниженими тарифами. Одержані гроші співучасники ділили між собою.

Збиток, заподіяний компанії «Укртелеком», становив 150 тис. грн.

Завдання 9

Калениченко, студент факультету інформатики одного з ВНЗ Львова, шляхом несанкціонованого доступу ознайомився з базою даних ТОВ «Світ без меж», що є провайдером послуг Інтернет, і встановив, що записи про число користувачів і їх рахунки захищено недостатньо. Скориставшись цим, він з метою безкоштовного отримання Інтернет-послуг, створив у цій базі рахунки, до яких вніс неправдиві відомості про попередню оплату за користування міжнародною комп'ютерною мережею Інтернет.

Безкоштовно працюючи в Інтернет, Калениченко заподіяв ТОВ «Світ без меж» шкоду в сумі 5000 грн. Після цього Калениченко розмістив на одному з сайтів оголошення про те, що за незначну плату він може забезпечити доступ до мережі Інтернет без оплати й обмеження часу, після чого був затриманий працівниками карного розшуку.

Завдання 10

Москаленко, співробітник підприємства «М-софтвер», яке займається виробництвом програмного забезпечення, звернувся до Ніконова по допомогу в розробленні нової програми.

Ніконов, бажаючи заподіяти шкоду підприємству «М-софтвер», розробив необхідну Москаленку програму і встановив у ній приховану функцію. Ця функція полягала в тому, що коли розроблена Ніконовим програма починає виконуватися на електронно-обчислювальній машині підприємства «М-софтвер», уся інформація, яка зберігається в ній, знищується.

Не знаючи цього, Москаленко встановив розроблену Ніконовим програму на одному з комп'ютерів «М-софтвер» і, запустивши її, знищив комп'ютерну інформацію, що належала цьому підприємству.

Завдання 11

Для отримання контракту на розроблення нового устаткування Коновалов, підприємець 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 Лотікову підкупити адміністратора комп'ютерної мережі НТП «Атол» і знайти фахівця з комп'ютерних технологій для знищення інформації в цій комп'ютерній мережі. Виконуючи розпорядження Коновалова, Лотіков зустрівся з інженером-програмістом Семченком, який погодився за винагороду проникнути в комп'ютерну мережу НТП «Атол» і знищити інформацію, що там обробляється. Після цього Лотіков одержав згоду Мельникова, адміністратора комп'ютерної мережі НТП «Атол», за винагороду знищити сліди проникнення Семченка до комп'ютерної мережі.

У призначений день Семченко здійснив несанкціоноване втручання в роботу комп'ютерної мережі НТП «Атол» і, знищивши інформацію, сповістив про це Коновалова. Останній зв'язався з Мельниковим, який згідно з домовленістю знищив сліди несанкціонованого втручання Семченка.

Завдання 12

Лейкіна у Києві придбала підроблені паспорт, трудову книжку і диплом про вищу економічну освіту. Приїхавши до Луганська, вона за цими документами влаштувалася на роботу в банк «Золо-

тий кредит». Пропрацювавши шість місяців і вивчивши роботу автоматизованої системи переказу платежів, вона вирішила вчинити незаконне заволодіння майном. З цією метою ввійшла в змову зі співробітником операційного відділу банку «Меркурій» Діденком, який допоміг Лейкіній відкрити розрахунковий рахунок і пообіцяв перевести в готівку гроші з нього в разі їх надходження.

В обумовлений час Лейкіна, використовуючи автоматизовану систему переказу платежів банку «Золотий кредит», перевела 300 тис. грн. на свій рахунок у банку «Меркурій». Під час спроби перевести в готівку гроші Лейкіну і Діденка було затримано співробітниками ДСБЕЗ.

Завдання 13

Трушкін працював програмістом у ТОВ «Азарт», основним видом діяльності якого була організація азартних ігор в мережі Інтернет. Скориставшись тим, що йому було надано доступ до програмного забезпечення ТОВ «Азарт», він скопіював його, проаналізував роботу цього забезпечення на своєму персональному комп'ютері та розробив спеціальну програму, яка давала змогу незаконно змінювати інформацію про гравців та їх ставки. Після цього він запустив розроблену програму на своєму робочому місці та вніс неправдиві відомості до бази даних ТОВ «Азарт», на підставі яких його сестра, Володіна, незаконно отримала 5346 грн. «виграшу».

Завдання 14

Рінатов, системний адміністратор ВАТ «Spyder», яке надавало населенню послуги доступу до мережі Інтернет, незаконно скопіював базу даних, що належала цій організації, у якій містилися відомості про логіни та паролі клієнтів. Потім запропонував цю базу даних Ігнатову, який придбав її за 400 грн.

Ігнатов, використовуючи відомості з бази даних, протягом трьох місяців незаконно отримував послуги доступу до мережі Інтернет від імені та за рахунок клієнтів ВАТ «Spyder». Під час, коли він здійснював доступ до мережі від імені конкретних клієнтів, останні не мали можливості отримати доступ до Інтернету.

Завдання 15

Приватний підприємець Комков придбав у невстановленої особи спеціальний технічний засіб, який надавав можливість знищувати інформацію про вартість реалізованої продукції з пам'яті

електронної контрольно-касової машини. З метою ухилення від сплати податків він протягом трьох місяців наприкінці кожного робочого дня, використовуючи цей технічний засіб, знищував у контрольно-касовій машині, розташованій у його власному продовольчому магазині, інформацію про реалізовану продукцію.

Завдання 16

Студент факультету інформатики одного з вузів Запоріжжя Лодкін розробив «троянську» комп'ютерну програму, яка будучи розміщеною на певному сайті, самостійно, без відома користувача, копіювалася на комп'ютер, з якого був отриманий доступ до цього сайту. Крім того, відповідно до цієї програми кожний комп'ютер, на якому вона встановлювалася, 1 вересня 2006 р. о 9:00 починав надсилати запити на офіційний сайт факультету, на якому навчався Лодкін. 1 травня 2006 р. він, скориставшись тим, що працював програмістом у місцевій газеті, незаконно розмістив дану програму на сайті цього видання. Протягом травня-серпня 2006 р. цей сайт відвідало 10 тисяч користувачів, на комп'ютері кожного з них автоматично була встановлена програма, яку розробив Лодкін. 1 вересня 2006 р. офіційний сайт факультету був недоступний до використання, оскільки ресурси сервера було вичерпано для опрацювання запитів, що надсилалися програмою Лодкіна.

Завдання 17

Дмитренка було звільнено з банку «Директ». Обурившись на адміністрацію банку, він зі свого домашнього комп'ютера через мережу Інтернет отримав доступ до бази даних клієнтів банку. Ця база містила інформацію про паспортні дані клієнтів, пін-коди та номери їх дебетних і кредитних карток. Дмитренко скопіював цю базу та розмістив її для загального доступу на одному з популярних сайтів.

Рекомендована література

Нормативні акти

1. Кримінальний кодекс України від 5 квітня 2001 року.
2. Закон України «Про державну таємницю» від 21 січня 1994 року.
3. Закон України «Про внесення змін до Кримінального кодексу України щодо відповідальності за незаконне втручання в роботу мереж електрозв'язку» від 5 червня 2003 року.
4. Закон України «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» від 23 грудня 2004 року.
5. Закон України «Про електронний цифровий підпис» від 22 травня 2003 року.
6. Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 року.
7. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31 травня 2005 року.
8. Закон України «Про Концепцію Національної програми інформатизації» від 4 листопада 1998 року.
9. Закон України «Про Національну програму інформатизації» від 4 лютого 1998 року.
10. Закон України «Про інформацію» від 2 листопада 1992 року.
11. Закон України «Про Національну систему конфіденційного зв'язку» від 10 січня 2002 року.
12. Закон України «Про телекомунікації» від 18 листопада 2003 року.
13. 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».
14. Указ Президента України № 1229/99 від 27 вересня 1999 року «Про Положення про технічний захист інформації в Україні».

15. Постанова Кабінету Міністрів України № 208 від 24 лютого 2003 року «Про заходи щодо створення електронної інформаційної системи «Електронний Уряд».
16. Постанова Кабінету Міністрів України № 3 від 4 січня 2002 року «Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади».
17. Постанова Кабінету Міністрів України № 1433 від 10 вересня 2003 року «Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади».
18. Постанова Кабінету Міністрів України № 522 від 12 квітня 2002 року «Про затвердження Порядку підключення до глобальних мереж передачі даних».
19. Постанова Кабінету Міністрів України № 1126 від 8 жовтня 1997 р. «Про затвердження Концепції технічного захисту інформації в Україні».
20. Розпорядження Кабінету Міністрів України № 259-р від 5 травня 2003 р. «Про затвердження Концепції формування системи національних електронних інформаційних ресурсів».
21. ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. Від 01.07.94.
22. ДСТУ 2938-94 Системи оброблення інформації. Основні положення. Терміни та визначення. Від 01.01.96.
23. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. Від 01.01.1998.

Монографії, автореферати дисертацій, навчальні посібники та довідники

1. *Батурин Ю. М.* Проблемы компьютерного права.– М.: Юридическая литература, 1991.– 271 с.
2. *Батурин Ю. М., Жодзишский А. М.* Компьютерная преступность и компьютерная безопасность.– М.: Юридическая литература, 1991.– 160 с.
3. *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.
4. *Біленчук П. Д., Романюк Б. В., Цимбалюк В. С.* та ін. Комп'ютерна злочинність:. Навчальний посібник.– К.: Атіка, 2002.– 204 с.

5. *Бутузов В. М., Останець С. Л., Шеломенцев В. П.* Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Науково-практичний коментар.– К.: Друкарня МВС України, 2005.– 86 с.

6. *Венгеров А. Б.* Право и информатика в условиях автоматизации управления (Теоретические вопросы).– М. Юридическая литература, 1978.

7. *Вехов В. В.* Компьютерные преступления: Способы совершения и раскрытия / Под ред. акад. Б. П. Смагоринского.– М.: Право и Закон, 1996.– 82 с.

8. *Вехов В. Б., Голубев В. А.* Расследование компьютерных преступлений в странах СНГ: Монография / Под ред. засл. деят. науки РФ, д-ра юрид. наук, проф. Б. П. Смагоринского.– Волгоград: ВА МВД России, 2004.– 304 с.

9. *Воройский Ф. С.* Систематизированный толковый словарь по информатике (Вводный курс по информатике и вычислительной технике в терминах).– М.: Киберия, 1998.

10. *Законодавство* про кримінальну відповідальність за «комп'ютерні» злочини: науково-практичний коментар і шляхи вдосконалення / А. А. Музика, Д. С. Азаров.– К.: Вид. Паливода А. В., 2005.– 120 с.– Бібліогр.: 108–119.

11. *Гаврилов О. А.* Информатизация правовой системы России. Теоретические и практические проблемы.– М., 1998.

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

13. *Голубєв В. О., Гавловський В. Д., Цимбалюк В. С.* Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Навчальний посібник / За заг. ред. д-ра юрид. наук, проф. Р. А. Калюжного.– Запоріжжя: ГУ «ЗІДМУ», 2002.– 292 с.

14. *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.

15. *Коваленко М. М.* Комп'ютерні віруси і захист інформації.– К.: Наукова думка, 1999.– 268 с.

16. *Кураков Л. П., Смирнов С. Н.* Информация как объект правовой защиты.– М.: Гелиос, 1998.– 240 с.

17. *Орлов С. О.* Кримінально-правова охорона інформації в комп'ютерних системах та телекомунікаційних мережах: Автореф. дис... канд. юрид. наук: 12.00.08 / Нац. ун-т внутр. справ.– Х., 2004.– 20 с.

18. *Першиков В. И., Савинков В. М.* Толковый словарь по информатике.– М.: Финансы и статистика, 1991.– 543 с.

19. *Полевой Н. С.* и др. Правовая информатика и кибернетика: Учебник.– М.: Юридическая литература, 1993.

20. *Ракитов А. И.* Философия компьютерной революции.– М.: Политиздат, 1991.– 260 с.

21. *Розенфельд Н. А.* Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: Автореф. дис... канд. юрид. наук: 12.00.08 / НАН України. Ін-т держави і права ім. В. М. Корецького.– К., 2003.– 17 с.

22. *Салтевський М. В.* Основи методики розслідування злочинів, скоєних з використанням ЕОМ: Навчальний посібник.– Х.: Нац. юрид. акад. України, 2000.– 35 с.

23. *Скоромников К. С.* Компьютерное право Российской Федерации.– М.: Изд-во МНЭПУ, 2000.

24. *Словарь* по кибернетике / Под ред. акад. В. М. Глушкова.– К.: Главная редакция Украинской Советской энциклопедии, 1979.– 420 с.

25. *Шилан Н. Н., Кривонос Ю. М., Бирюков Г. М.* Компьютерные преступления и проблемы защиты информации: Монография.– Луганск: РИО ЛИВД, 1999.– 60 с.

Статті та тези доповідей

1. *Азаров Д. С.* Нові зміни до розділу XVI Особливої частини Кримінального кодексу України – нові проблеми // Юридичний вісник України.– 2005.– № 6.– С. 28–32.

2. *Ахмадулин Д. К.* Опыт расследования уголовного дела о хищении денежных средств с использованием несовершенства компьютерной программы // Информационный бюллетень следственного комитета МВД России.– 1998.– № 2 (95).– С. 75–79.

3. *Венгеров А. Б.* Категория «информация» в понятийном аппарате юридической науки // Советское государство и право.– 1977.– № 10.

4. *Вехов В.* Документы на машинном носителе // Законность.– 2004.– № 2.– С. 18–20.

5. *Вехов В. Б.* Компьютерная информация как объект криминалистического исследования // Воронежские криминалистические чтения: Сб. науч. трудов. Вып. 6 / Под ред. О. Я. Баева.– Воронеж: Изд-во Воронеж. гос. ун-та, 2005.– С. 51–70.

6. *Гончаров Д.* Квалификация хищений, совершаемых с помощью компьютеров // Законность.– 2001.– № 11.– С. 31–32.

7. *Карчевський М. В.* Кримінальна відповідальність за незаконне втручання в роботу мереж електрозв'язку (нова редакція ст. 361 КК України) // Вісник Луганської академії внутрішніх справ імені 10-річчя незалежності України.– 2004.– № 2.– С. 220–234.

8. *Карчевський М. В.* Проблеми гармонізації українського та міжнародного законодавства про комп'ютерні злочини // Вісник Луганського державного університету внутрішніх справ.– 2005.– № 4.– С. 122–133.

9. *Кириченко С. А.* Из практики раскрытия и расследования компьютерных преступлений // Информационный бюллетень следственного комитета МВД России.– 1998.– № 2 (95).– С. 61–63.

10. *Краснова Л. Б.* Понятие уголовно-релевантного компьютерного объекта и его классификация // Воронежские криминалистические чтения: Сб. науч. трудов. Вып. 4 / Под ред. О. Я. Баева.– Воронеж: Изд-во Воронеж. гос. ун-та, 2003.– С. 170–176.

11. *Кузнецов Н. А., Мусхелишвили Н. Л., Шрейдер Ю. А.* Информационное взаимодействие как объект научного исследования // Вопросы философии.– 1999.– № 2.– С. 77–87.

12. *Лісовий В.* «Комп'ютерні» злочини: питання кваліфікації // Право України.– 2002.– № 2.– С. 86–88.

13. *Менжега М. М.* Некоторые дискуссионные вопросы понятия и содержания статьи 273 УК РФ: (создание, использование и распространение вредоносных программ для ЭВМ) // Следователь.– 2004.– № 3.– С. 9–12.

14. *Мещеряков В. А.* Состав, структура и особенности криминалистической характеристики преступлений в сфере компьютерной информации // Воронежские криминалистические чтения. Вып. 2 / Под ред. О. Я. Баева.– Воронеж: Изд-во Воронеж. гос. ун-та, 2001.– С. 137–154.

15. *Северин В. А.* Правовое регулирование информационных отношений // Вестник МГУ. Серия 11. Право.– 2000.– № 5.

16. *Семенов Г. В.* Криминалистическая классификация преступлений против информации в системе сотовой связи // Воронежские криминалистические чтения. Вып. 2 / Под ред. О. Я. Баева.– Воронеж: Изд-во Воронеж. гос. ун-та, 2001.– С. 127–136.

17. *Семенов Г. В.* Телекоммуникационное мошенничество: введение в проблему // Воронежские криминалистические чтения. Вып. 1 / Под ред. О. Я. Баева.– Воронеж: Изд-во Воронеж. гос. ун-та, 2000.– С. 100–106.

18. *Семилетов С. И.* Информация как особый нематериальный объект права // Государство и право.– 2000.– № 5.– С. 67–74.

19. *Снігерьов О. П., Голубєв В. О.* Проблеми класифікації злочинів у сфері комп'ютерної інформації // Вісник Університету внутрішніх справ.– Х., 1999.– Вип. 5.– С. 25–28.

20. *Тарасенко Ф. П.* К определению понятия «информация» в кибернетике // Вопросы философии.– 1963.– № 4.– С. 76–84.

21. *Терещенко Л. К.* Информация и собственность // Защита прав создателей и пользователей программ для ЭВМ и баз данных (комментарий российского законодательства).– М., 1996.

22. *Украинцев Б. С.* Информация и отражение // Вопросы философии.– 1963.– № 2.– С. 26–38.

23. *Чечко Л.* «Компьютерные» хищения // Российская юстиция.– 1996.– № 5.– С. 45.

24. *Ярыш В. Н., Ходжейса В. П., Францифоров Ю. В.* Расследование преступлений в сфере высоких технологий // Следователь.– 2003.– № 8.– С. 41–43.

Джерела мережі Інтернет

1. www.dstszi.gov.ua – Державна служба спеціального зв'язку та захисту інформації України.

2. www.crime-research.ru – Центр исследования компьютерной преступности.

3. www.cyber-crimes.ru – Федеральный правовой портал. Компьютерные преступления: квалификация, расследование, профилактика.

4. www.cyberpol.ru – Компьютерная преступность и борьба с нею.

5. www.bezpeka.com – Официальный сайт «Центра информацинной безопасности».

6. www.cybercrime.gov – Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice.

7. www.dcfl.gov – U.A. Department of Defense Cyber Crime Center (DC3).

8. www.cert.org – CERT (organization devoted to ensuring that appropriate technology and systems management practices are used to resist attacks on networked systems and to limiting damage and ensure continuity of critical services in spite of successful attacks, accidents, or failures).

Додатки

Додаток 1

КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ

(Витяги)

Розділ XVI

ЗЛОЧИНИ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

(Розділ із змінами, внесеними згідно із законами України від 05.06.2003 р. № 908-IV, від 23.12.2004 р. № 2289-IV)

Стаття 361. **Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку**

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації,–

карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,–

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

Примітка. Значною шкодою у статтях 361–363[1], якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

(У редакції законів України від 05.06.2003 р. № 908-IV, від 23.12.2004 р. № 2289-IV)

Стаття 361-1. **Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут**

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку,–

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк, з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,–

караються позбавленням волі на строк до п'яти років з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

(Доповнено статтею 361-1 згідно із Законом України від 23.12.2004 р. № 2289-IV)

Стаття 361-2. **Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації**

1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства,–

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,–

караються позбавленням волі на строк від двох до п'яти років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

(Доповнено статтею 361-2 згідно із Законом України від 23.12.2004 р. № 2289-IV)

Стаття 362. **Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї**

1. Несанкціоновані зміни, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї,–

караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи.

2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації,–

караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,–

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

(У редакції Закону України від 23.12.2004 р. № 2289-IV)

Стаття 363. **Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється**

Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію,–

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

(У редакції Закону України від 23.12.2004 р. № 2289-IV)

Стаття 363-1. **Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку**

1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку,–

карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду,–

караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено масове розповсюдження повідомлень електрозв'язку, які є власністю винної особи.

(Доповнено статтею 363-1 згідно із Законом України від 23.12.2004 р. № 2289-IV)

Додаток 2

ПРОЕКТ ЗАКОНУ УКРАЇНИ
Про внесення змін до Кримінального та Кримінально-процесуального кодексів України

Верховна Рада України ПОСТАНОВЛЯЄ:

І. Внести до Кримінального та Кримінально-процесуального кодексів України такі зміни:

1. У Кримінальному кодексі України

1) назву розділу XVI викласти в такій редакції «**Злочини у сфері використання комп'ютерних систем та мереж електрозв'язку**»;

2) статті 361–361-2 викласти в такій редакції:

Стаття 361. **Несанкціоновані дії з комп'ютерними даними**

1. Несанкціоновані ознайомлення, копіювання, перехоплення, знищення, зміна, блокування комп'ютерних даних, спотворення процесу обробки комп'ютерних даних або порушення встановленого порядку їх маршрутизації,–

карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоновані дії, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,–

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоновані дії, які є власністю винної особи.

3. Дії, передбачені частиною першою або другою, якщо вони спричинили тяжкі наслідки,–

караються позбавленням волі на строк від п'яти до восьми років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоновані дії, які є власністю винної особи.

Примітка. 1. У статтях 361–62 та 363-1, 363-2 повторним визнається злочин, вчинений особою, що раніше вчинила будь-який із злочинів, передбачених цими статтями цього Кодексу.

2. Значною шкодою у статтях 361–363-1, 363-2, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

3. Тяжкими наслідками у статтях 361–363-1, 363-2, якщо вони полягають у заподіянні матеріальних збитків, вважаються такі, які у п'ятсот і більше разів перевищують неоподатковуваний мінімум доходів громадян.

Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів,–

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк, з конфіскацією шкідливих програмних чи технічних засобів, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,–

караються позбавленням волі на строк до п'яти років з конфіскацією шкідливих програмних чи технічних засобів.

3. Дії, передбачені частиною першою або другою, якщо вони спричинили тяжкі наслідки,–

караються позбавленням волі на строк від п'яти до восьми з конфіскацією шкідливих програмних чи технічних засобів.

Стаття 361-2. Несанкціоновані збут або розповсюдження комп'ютерної інформації з обмеженим доступом

1. Несанкціоновані збут або розповсюдження комп'ютерної інформації з обмеженим доступом,–

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,–

караються позбавленням волі на строк від двох до п'яти років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

3. Дії передбачені частиною першою або другою, якщо вони спричинили тяжкі наслідки,–

караються позбавленням волі на строк від п'яти до восьми років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи»;

3) доповнити статтею 361-3 такого змісту:

Стаття 361-3. Несанкціонований доступ до комп'ютерної інформації

Незаконне одержання можливості ознайомлюватися, знищувати, перекручувати або блокувати комп'ютерні дані, що мають організаційні, технічні або програмні засоби захисту,–

карається обмеженням волі на строк до трьох років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціонований доступ»;

4) статті 362–363-1 викласти в такій редакції:

Стаття 362. Несанкціоновані дії з комп'ютерними даними, вчинені особою, яка має правомірний доступ до них у зв'язку з займаною посадою або спеціальними повноваженнями

1. Несанкціоновані зміна, знищення або блокування комп'ютерних даних, вчинені особою, яка має до них правомірний доступ у зв'язку з займаною посадою або спеціальними повноваженнями,–

караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років з конфіскацією програмних або технічних засобів, за

допомогою яких було вчинено несанкціоновані зміна, знищення або блокування даних, які є власністю винної особи.

2. Несанкціоновані перехоплення або копіювання комп'ютерних даних, якщо це призвело до їх витоку, вчинені особою, яка має правомірний доступ до комп'ютерних даних у зв'язку з займаною посадою або спеціальними повноваженнями,–

караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання даних, які є власністю винної особи.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,–

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з даними, які є власністю винної особи.

4. Дії, передбачені частиною першою, другою або третьою цієї статті, якщо вони спричинили тяжкі наслідки,–

караються позбавленням волі на строк від п'яти до восьми років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з даними, які є власністю винної особи.

Стаття 363. **Порушення правил експлуатації комп'ютерних систем чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється**

Порушення правил експлуатації комп'ютерних систем чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за дотримання вимог інформаційної безпеки,–

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

Стаття 363-1. **Розповсюдження спаму**

1. Умисне масове розповсюдження спаму яке заподіяло значну шкоду,–

карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони спричинили тяжкі наслідки,–

караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено масове розповсюдження спаму, які є власністю винної особи.

3. Дії, передбачені частиною першою або другою, якщо вони спричинили тяжкі наслідки,–

караються позбавленням волі на строк від п'яти до восьми років, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено масове розповсюдження спаму, які є власністю винної особи»;

5) доповнити статтею 363-2 такого змісту:

«Стаття 363-2. **Несанкціоноване втручання в роботу мереж електрозв'язку**

1. Несанкціоноване втручання в роботу мереж електрозв'язку, яке заподіяло істотну шкоду,–

карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

2. Те саме діяння, вчинене повторно або за попередньою змовою групою осіб, якщо воно спричинило тяжкі наслідки,–

карається позбавленням волі на строк від трьох до восьми років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи».

2. Частини другу і третю статті 112 Кримінально-процесуального кодексу України після цифр «361-2» доповнити цифрами «361-3», а після цифр «363-1» – цифрами «363-2».

II. Цей Закон набирає чинності з дня його опублікування.

Алфавітно-предметний покажчик

Навчальне видання

ЗЛОЧИНИ У СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРНОЇ ТЕХНІКИ

КАРЧЕВСЬКИЙ Микола Віталійович

Головний редактор *Гайдук Н. М.*
Редактори: *Голубовська Л. В., Пипченко В. Я.*
Коректор *Сікорська Л. Л.*
Художнє оформлення та комп'ютерна верстка *Остапенко В. С.*

Підписано до друку 30.IX 2009 р. Формат 60×84/16. Папір офсетний. Гарнітура Тип Таймс. Друк офсетний. Умовн. друк. арк. 9,76. Наклад 500 пр. Зам. № 2068

Оригінал-макет виготовлений ТОВ «Атіка», 04060 Київ-60, вул. М. Берлинського, 9.
Свідоцтво про видавничу діяльність і розповсюдження видавничої продукції:
Серія ДК № 216 від 11.X 2000 р.,
видане Державним комітетом інформаційної політики, телебачення та радіомовлення України.

Надруковано ПП «Рута»
10014 м. Житомир, вул. М. Бердичівська, 17-а
Реєстраційне свідоцтво серія ЖТ № 2 від 24.12.2001 р