Стаття 361. Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

1. Незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж, що призвело до перекручення чи знищення комп'ютерної інформації або носіїв такої інформації, а також розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в ці машини, системи чи комп'ютерні мережі і здатних спричинити перекручення, або знищення комп'ютерної інформації чи носіїв такої інформації, а так само незаконне втручання в роботу мереж електрозв'язку, що призвело до знищення, перекручення, блокування інформації або до порушення встановленого порядку її маршрутизації, — караються штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на той самий строк.

2. Ті самі дії, якщо вони заподіяли істотну шкоду або вчинені повторно чи за попередньою змовою групою осіб, — караються штрафом від ста до чотирьохсот неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до п'яти років, або позбавленням волі на строк від трьох до п'яти років. Примітка. Під істотною шкодою, якщо вона полягає в завданні матеріальних збитків, слід розуміти таку шкоду, яка в триста і більше разів перевищує неоподатковуваний мінімум доходів громадян.

(У редакції Закону України від 05.06.2003 р. № 908-IУ)

1. Науково-технічний прогрес неможливий без широкомасштабного впро-вадження в управлінську діяльність, у різні сфери науки, техніки і вироб-ництва електронно-обчислювальної техніки і мереж електрозв'язку. Це вима-гає розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності. У цьому відношенні базовими нормативними актами в Україні є: закони України «Про захист інформації в автоматизованих системах» від 5 липня 1994 р. (ВВР. — 1994. — № 31), «Про зв'язок» від 16 травня 1995 р. (в редакції від 5 червня 2003 р.) (ВВР. — 1995. — № 20); «Положення про технічний захист інформації в Україні», затверджене Указом Президента України від 29 вересня 1999 р. № 1229, та ін.

У розділі XVI КК у статтях 361, 362, 363 передбачена відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), їх систем чи комп'ютерних мереж та мереж електрозв'язку.

2. Родовий об'єкт — інформаційна безпека, безпосередній — нормальне функціонування електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж, комп'ютерної інформації та мереж електрозв'язку.

3. Предмет злочину: 1) електронно-обчислювальна машина (ЕОМ) — комп'ютер — комплекс технічних засобів, призначених для автоматичної обробки інформації в процесі вирішення обчислювальних та інформаційних завдань;

2) автоматизовані комп'ютерні системи (АКС) — сукупність взаємопов'язаних ЕОМ, периферійного устаткування та програмного забезпечення, призначених для автоматизації прийому, збереження, обробки, пошуку та видачі інформації споживачам. Комп'ютерні системи можуть бути регіонального і галузевого характеру; 3) комп'ютерні мережі (мережа ЕОМ) — це об'єднання кількох комп'ютерів (ЕОМ) і комп'ютерних систем, взаємопов'язаних і розподілених за фіксованою територією та орієнтованих на колективне використання загальносітьових ресурсів. Комп'ютерні мережі припускають спільне використання ресурсів обчислювальних центрів (ОЦ), запуск загальних програм, що входять до комп'ютерних систем; 4) носії комп'ютерної інформації — фізичні об'єкти, машинні носії, призначені для постійного збереження, переносу та обробки комп'ютерної інформації. До них належать гнучкі магнітні диски (дискети), жорсткі магнітні диски (вінчестери), касетні магнітні стрічки (стримери), магнітні барабани, магнітні карти та ін.; 5) комп'ютерна інформація — це текстова, цифрова, графічна чи інша інформація (дані, відомості) про осіб, предмети, події, явища, що існує в електронному вигляді, зберігається на відповідних електронних носіях (вінчестерах, дискетах, стримерах тощо) і може використовуватися, оброблятися чи змінюватися за допомогою ЕОМ (комп'ютерів); 6) мережі електрозв'язку — це сукупність засобів та споруд зв'язку, з'єднаних у єдиний технологічний процес забезпечення інформаційного обміну — передачі, випромінювання або прийому знаків, сигналів письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах. До них належать, зокрема, телефонний, телеграфний, телетайпний та факсимільний зв'язок. Предмети мережі електрозв'язку включають телефони, факси, телетайпи, телеграфи, інші апарати, пристрої і обладнання мереж електрозв'язку, призначені для передачі і обміну інформацією. До предмета цього злочину належить також і інфор-мація, що є в обігу мереж електрозв'язку.

4. Об'єктивна сторона злочину, що розглядається, полягає в трьох фор-мах: 1) у незаконному втручанні в роботу автоматизованих машин (комп'ютерів), їх систем або комп'ютерних мереж; 2) у розповсюдженні комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в ці машини (ЕОМ), системи або комп'ютерні мережі і здатних спричинити перекручування або знищення комп'ютерної інформації чи носіїв такої інформації; 3) у незаконному втручанні в роботу мереж електрозв'язку.

1) Незаконне втручання в роботу автоматизованих машин (комп'ютерів), їх систем або комп'ютерних мереж характеризується проникненням у ці ма-шини, їх системи чи мережі і здійсненням дій, що виявляються в порушенні режиму роботи ЕОМ, призупиненні (частковому або повному) їх роботи. Таке втручання повинне бути незаконним, тобто особа не мала ні дійсного, ні передбачуваного права на втручання в роботу ЕОМ. При цьому електронно-обчислювальні машини не належать винному ні на праві власності, ні на якій-небудь іншій законній підставі (наприклад, на умовах оренди). Тут завжди має місце злам і проникнення (вторгнення) у програму чужого комп'ютера, системи або мережі ЕОМ. Способи втручання в роботу електронно-обчислювальних машин можуть

бути різними: шляхом виявлен-ня слабких місць у захисті, шляхом автоматичного перебору абонентських номерів («угадування коду»), дії «хакерів», з'єднання з тим чи іншим комп'ютером, підключеним до телефонної мережі, використання чужого імені (пароля) за допомогою використання помилки в логіці побудови програми та ін.

Наслідками такого діяння повинне бути перекручення чи знищення комп'ютерної інформації або носіїв такої інформації. Перекручення — це зміна змісту або форми інформації, закладеної в носії, коли можливість використання чи відновлення цієї інформації чи її фрагментів істотно утруднена. Знищення комп'ютерної інформації виявляється в такій її зміні, коли її споживання, використання або відновлення неможливе. Знищення носіїв комп'ютерної інформації полягає у руйнівному впливі на них (механічному, електронному), внаслідок чого вони приходять у повну непридатність і не можуть бути використані за своїм цільовим призначенням (наприклад, знищення вінчестера, дискети, стримера тощо).

2) Розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в ці машини (ЕОМ), системи або комп'ютерні мережі і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації. Комп'ютерний вірус — це шкідлива програма, що «інфікує» носія комп'ютерної інформації, вставляючи в нього власні копії і зміни. Програма, що містить комп'ютерний вірус, має реальну і дуже високу ступінь можливості знищення, блокування, модифікації комп'ютерної інформації, порушення роботи ЕОМ, їх систем або мереж. Тому поширення комп'ютерного вірусу («злам» комп'ютерних систем і мереж за допомогою «вірусної атаки») становить підвищену небезпеку для суспільних відносин у сфері комп'ютерної безпеки.

Засобами здійснення цього злочину є програмні і технічні засоби. Програма-вірус — це спеціально створена програма, яка здатна мимовільно приєднуватися до інших програм (тобто «заражати» їх) і при запуску вико-нувати різні небажані дії: зіпсування файлів і каталогів, перекручування результатів обчислення, засмічення чи стирання пам'яті, створення перешкод у роботі ЕОМ. Технічні засоби — це електронно-обчислювальні машини (комп'ютери) і їх системи, за допомогою яких вірусні програми протиправне вводяться в базу даних ЕОМ (комп'ютерів) і їхніх систем або мереж. До технічних засобів слід відносити й інші пристосування, які так само, як і програмні засоби повинні бути призначені (мати цільове призначення) для незаконного проникнення в електронно-обчислювальні машини (комп'ютери) і їх системи або мережі і здатні спричинити перекручення чи знищення комп'ютерної інформації або носіїв такої інформації.

3) Незаконне втручання в роботу мереж електрозв'язку з об'єктивної сторони характеризується проникненням, вторгненням у мережі електрозв'язку, що завжди пов'язане з порушенням режиму роботи цих систем чи їх складових частин. Це втручання повинне бути незаконним — системи електрозв'язку належать певному власнику — юридичній або фізичній особі і на втручання в їх

роботу винна особа не має ні дійсного, ні передбачуваного права. Способи незаконного вторгнення в роботу мереж електрозв'язку можуть бути різними: підключення до ліній зв'язку, використання різних технічних пристроїв («жучків») для прослуховування і фіксування інформації, яка є в обігу систем електрозв'язку та ін.

Наслідками такого діяння має бути: знищення, перекручення, блокування інформації або порушення встановленого порядку її маршрутизації. Зміст понять «знищення» і «перекручення» інформації мереж електрозв'язку тотожні поняттям «знищення» і «перекручення» комп'ютерної інформації (див. коментар п. 1 цієї статті). Блокування інформації — це таке порушення інформаційних потоків мереж електрозв'язку, внаслідок якого суб'єкт-передавач інформації не може донести інформацію до абонента, а той не може цієї інформації отримати. Маршрутизація інформації — це порушення обрання послідовності вузлів мережі передачі інформації, якою інф-ія передається від джерела до приймача інф-ції.

Злочин вважається закінченим з моменту настання одного із зазначених наслідків — перекручення чи знищення комп'ютерної інформації, знищення хоча б одного носія такої інформації, при першій формі, при другій — поширення (введення) у базу даних ЕОМ (комп'ютерів), їх систем чи мереж комп'ютерного вірусу, а при третій — з моменту знищення, перекручення, блокування інформації або з моменту порушення встановленого порядку її маршрутизації.

5. Суб'єктивна сторона злочину — умисел (прямий чи непрямий).

6. Суб'єкт злочину — особа фізична, осудна, що досягла 16-річного віку.

7. У частині 2 ст. 361 КК передбачена відповідальність за ті ж дії, що спричинили істотну шкоду або вчинені повторно чи за попередньою змовою групою осіб.

Істотна шкода визначається багатьма обставинами: вартістю комп'ютерної інформації та її носіїв; майнового збитку, заподіяного власнику внаслідок неможливості використання знищеної чи перекрученої комп'ютерної інформації чи її носіїв; розміром витрат, необхідних для відновлення комп'ютерної інформації чи її носіїв. Істотна шкода — поняття оціночне і воно повинне уточнюватися (конкретизуватися) у кожному конкретному випадку з урахуванням усіх обставин справи, у тому числі з урахуванням матеріального стану потерпілого та ін.

Повторність — див. ст. 32 КК і коментар до неї.

Здійснення злочину за попередньою змовою групою осіб — див. ст. 28 КК і коментар до неї. Тут слід враховувати, що співучасники можуть діяти не тільки як виконавці (співвиконавці), а й із розподілом ролей. Наприклад, одна особа розробляє технічні програми, що містять вірус, або виготовляє інші технічні засоби, друга їх тиражує, третя здійснює акт незаконного втручання

(вторгнення) у роботу ЕОМ. Дії виконавця охоплюються ч. 2 ст. 361 КК, інші співучасники несуть відповідальність за ст. 27 і ч. 2 ст. 361 КК.

8. Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж може бути іноді як спосіб здійснення інших злочинів, наприклад: диверсії (ст. 113 КК), шпигунства (ст. 114 КК), шахрайства (ст. 190 КК), незаконних дій з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення (ст. 200 КК), незаконного збирання з метою використання або використання відомостей, що становлять комерційну таємницю (ст. 231 КК) та ін. У подібних випадках вчинене підлягає кваліфікації за сукупністю: за ст. 361 КК і статтею, що передбачає відповідальність за конкретний злочин, способом здійснення якого було незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.