Розділ XVIII Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

§1. Поняття злочинів у сфері використання електронно- обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Науково-технічний прогрес неможливий без широкомасштабного впровадження в управлінську діяльність, у різні сфери науки, техні-ки і виробництва електронно-обчислювальної техніки і мереж електрозв'язку. Це вимагає розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності. У цьому відношенні базовими нормативними актами в Україні є: за-кони України: «Про захист інформації в інформаційно-телекому-нікаційних системах» від 5 липня 1994 р. (у редакції від 19 березня 2009 р.), «Про зв'язок» від 16 травня 1995 р. (у редакції від 5 червня 2003 р.), «Про телекомунікації» від 18 листопада 2003 р. (у редакції від 11 січня 2007 р.), а також низка підзаконних актів: «Положення про технічний захист інформації в Україні», затверджене Указом Прези-дента України від 27 вересня 1999 р. № 1229, наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 24 грудня 2001 р. № 76 «Про затвердження По-рядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах» та ін.

У статті 361 КК «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку», ст. 361^1 КК «Створен-ня з метою використання, розповсюдження або збуту шкідливих про-грамних чи технічних засобів, а також їх розповсюдження або збут», ст. 361^2 КК «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчис-лювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації», ст. 362 КК «Несанкціоновані дії з інформацією, яка оброблюється в електронно- обчислювальних машинах (комп'ютерах), автоматизованих систе-мах, комп'ютерних мережах або зберігається на носіях такої інфор-мації, вчинені особою, яка має право доступу до неї», ст. 363 КК «Порушення правил експлуатації електронно-обчислювальних ма-шин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту

інформації, яка в них оброблюється», ст. 363 [1] КК «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів) автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масо-вого розповсюдження повідомлень електрозв'язку» передбачена відповідальність за злочини у сфері використання електронно- обчислювальних машин (комп 'ютерів), їх систем чи комп'ютерних мереж та мереж електрозв' язку.

Родовий об'єкт — інформаційна безпека, безпосередній — нормаль-не функціонування електронно-обчислювальних машин (комп 'ютерів), автоматизованих систем, комп 'ютерних мереж, комп'ютерної інфор-мації та мереж електрозв'язку.

Предмет злочину: 1) електронно-обчислювальна машина (ЕОМ) — комп 'ютер — комплекс електронних технічних засобів, побудованих на основі мікропроцесорів і призначених для автоматичної обробки інформації при вирішенні обчислювальних та інформаційних завдань. ЕОМ складається, як правило, із трьох частин: системного блока, який включає в себе мікропроцесор та інші пристрої, необхідні для її робо-ти (накопичувачі даних, блок живлення тощо), клавіатури, за допо-могою якої вводяться в ЕОМ символи, та монітора, на якому відобра-жається текстова і графічна інформація; 2) автоматизовані системи (АС) — системи, що здійснюють автоматизовану обробку даних, до складу яких входять технічні засоби їх обробки (засоби обчислюваль-ної техніки і зв'язку), а також методи і процедури, програмне забез-печення. До складу АС входить принаймні одна ЕОМ та периферійні пристрої, що працюють на основі такої ЕОМ: принтер, сканер, модем, мережевий адаптер та ін.; АС включають у себе комп'ютерні мережі і мережі електрозв'язку; 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 орієн-тованих на колективне використання загальномережевих ресурсів. Комп'ютерні мережі передбачають спільне використання ресурсів об-числювальних центрів (ОЦ), запуск загальних програм, що входять до комп'ютерних систем; ЕОМ можуть включати дві чи більше автома-тизованих комп'ютерних системи (АКС) як сукупність взаємопов'язаних ЕОМ, периферійного устаткування та програмного забезпечення, при-значених для автоматизації прийому, збереження, обробки, пошуку та видачі інформації споживачам. Комп'ютерні системи можуть бути регіонального і галузевого характеру; 4) мережі електрозв'язку — це сукупність технічних засобів та споруд зв'язку, з'єднаних у єдиний технологічний процес забезпечення інформаційного обміну — марш-рутизації, комунікації, 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, теле-тайпний та факсимільний зв'язок. Предмети мережі електрозв'язку включають телефони, факси, телетайпи, телеграфи, інші апарати, при-строї і обладнання мереж електрозв'язку, призначені для передачі й обміну інформацією; 5) комп'ютерна інформація — це текстова, циф-рова, графічна чи інша інформація (дані, відомості) про

осіб, пред-мети, події, явища, що існує в електронному вигляді і знаходиться в ЕОМ, АС чи в комп'ютерній мережі, а також зберігається на відповід-них електронних носіях, до яких належать гнучкі магнітні диски (дис-кети), жорсткі магнітні диски (вінчестери), касетні магнітні стрічки (стримери), магнітні барабани, магнітні карти та ін. Інформація носіїв може використовуватися, оброблятися чи змінюватися за допомогою ЕОМ (комп'ютерів); 6) інформація, що передається мережами електрозв'язку (телекомунікаційними мережами) — будь-які відомос-ті, подані у вигляді сигналів, знаків, звуків, зображень чи в інший спосіб (телефонні повідомлення, радіо- та телепередачі тощо), у тому числі і за допомогою комп' ютера, якщо вона передається через мережі електрозв'язку.

Об'єктивна сторона цих злочинів може виражатися в активних діях (наприклад, при несанкціонованому втручанні в роботу електронно- обчислювальних машин (комп' ютерів), автоматизованих систем, комп 'ютерних мереж чи мереж електрозв'язку) — ст. 361 КК або в злочинній бездіяльності (наприклад, при порушенні правил експлуа-тації електронно-обчислювальних машин (комп'ютерів), автоматизо-ваних систем, комп'ютерних мереж чи мереж електрозв'язку або по-рядку чи правил захисту інформації, яка в них обробляється, — ст. 363 КК).

Для об'єктивної сторони деяких злочинів потрібно не тільки вчи-нення суспільно небезпечного діяння (умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адреса-тів), а й настання суспільно небезпечних наслідків — матеріальні склади злочинів: порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ч. 1 ст. 363^1 КК). В інших випадках розглядувані злочини сформульовані як склади зло-чинів з формальним складом (створення з метою використання, роз-повсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ч. 1 ст. 366 ^{1} КК).

Суб'єктивна сторона цих злочинів передбачає, як правило, умис-ну вину. Можлива і необережність — при порушенні правил експлуа-тації електронно-обчислювальних машин (комп'ютерів), автоматизо-ваних систем, комп'ютерних мереж чи мереж електрозв'язку або по-рядку чи правил захисту інформації, яка в них обробляється (ст. 363 КК).

Мотиви та цілі можуть бути різними — помста, прагнення до за- володіння інформацією. Якщо ж викрадення інформації вчиняється з корисливих мотивів і містить ознаки шахрайства, вчинене слід квалі-фікувати за сукупністю злочинів — за статтями 362 і 190

КК.

Суб'єкт злочину — особа фізична, осудна, що досягла 16-річного віку. У деяких випадках суб'єкт спеціальний — особа, яка відповідає за експлуатацію ЕОМ, автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку або повинна забезпечувати порядок чи виконан-ня правил захисту інформації, яка в них обробляється (ст. 363 КК).

---

§ 2. Види злочинів у сфері використання електронно-обчислювальних машин (комп' ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Несанкціоноване втручання в роботу електронно-обчислю вальних машин (комп' ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК). Об'єктивна сторона злочину, що розглядається, характеризується: 1) дією у вигляді несанкціонованого втручання в роботу електронно- обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; 2) суспільно небез-печними наслідками у формі: витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації; 3) причинним зв'язком між дією та зазначеними наслідками.

І. Несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку — це самочин-не, без дозволу власника або уповноваженої особи проникнення у вказані електронні системи чи мережі. При несанкціонованому втру-чанні особа протиправно отримує доступ до інформації, що зберіга-ється в ЕОМ та АС, на що вона не має ні дійсного, ні передбачуваного права. Електронно-обчислювальні машини чи їх мережі не належать винному ні на праві власності, ні на якій-небудь іншій законній під-ставі (наприклад, на умовах оренди). Тут завжди має місце злам і про-никнення (вторгнення) у програму чужого комп'ютера, системи або мережі ЕОМ. При втручанні в роботу ЕОМ, автоматизованих систем, комп

'ютерних мереж чи мереж електрозв'язку завжди має місце не-гативний вплив на нормальне функціонування цих систем і мереж, а також інформаційних процесів, що в них проходять. Ці дії протирічать охоронюваним законом правам і інтересам власника та заподіюють йому певну шкоду. Способи втручання в роботу вказаних систем і мереж можуть бути різними: шляхом виявлення слабких місць у за-хисті, шляхом автоматичного перебирання абонентських номерів («угадування коду»), дії «хакерів», з 'єднання з тим чи іншим комп'ютером, підключеним до телефонної мережі, використання чужо-го імені (пароля) за допомогою існуючої помилки в логіці побудови програми та ін., і не впливають на встановлення складу злочину (ст. 361 КК) як підстави кримінальної відповідальності. Але вони враховуються при оцінці суспільної небезпеки вчинення злочину і призначенні покарання.

II. Суспільно небезпечні наслідки. Розглядуваний злочин є злочи-ном з матеріальним складом. Для його наявності слід встановити не тільки вчинення діяння, а й настання хоча б одного з вказаних у законі наслідків: витоку, втрати, підробки, блокування інформації, спотворен-ня процесу обробки інформації або порушення встановленого порядку її маршрутизації.

Витік інформації має місце у випадках, коли вона стає відомою (доступною) хоча б одній особі, яка не має на це права, наприклад, у наслідок ознайомлення з її змістом, шляхом копіювання інформації та ін. При цьому власник не позбавляється інформації, яка йому нале-жить.

Втрата інформації — це припинення існування інформації віднос-но осіб, які мають право власності на неї. Втрата інформації може бути результатом її знищення, «викрадання», внаслідок якого власник по-збавляється належної йому інформації.

Підробка інформації — це дії, що призводять до перекручення (модифікації) змісту інформації, яка обробляється в ЕОМ чи АС, або створення інформації, що за змістом не відповідає дійсності (фальси-фікація інформації).

Блокування інформації має місце у випадках, коли внаслідок не-санкціонованого втручання в роботу ЕОМ та АС власник чи уповно-важена особа не має доступу до інформації, не отримує її і не має можливості користування нею. Тут може мати місце приховування чи стримування інформації для запобігання користуванню нею в процесі її обробки.

Спотворення процесу обробки інформації — це зміна послідовнос-ті оброблення інформації, порядок якої встановлюється власником ЕОМ чи АС. Тут може порушуватись порядок: збирання, ведення, записування, перетворення, зчитування, знищення, реєстрація, прийнят-тя, отримання, передавання інформації. Унаслідок вказаного спотво-рення процесу обробки інформації одержується інший результат, ніж очікувався.

Порушення встановленого порядку маршрутизації — це проти-правна, внаслідок несанкціонованого втручання, зміна адресата інфор-мації, яка передається телекомунікаційними каналами. Унаслідок по-рушення порядку маршрутизації адресат не отримує інформації, яка була для нього направлена, або таку інформацію отримують і інші особи, яким ця інформація не була адресована.

III. Для наявності об'єктивної сторони розглядуваного злочину слід встановити причинний зв'язок між несанкціонованим втручанням у роботу ЕОМ чи АС і хоча б одним із суспільно небезпечних наслідків, в альтернативі вказаних у диспозиції ч. 1 ст. 361 КК.

Суб 'єктивна сторона злочину характеризується умисною формою вини. Мотив і мета злочину — різні і для кваліфікації значення не мають.

Суб 'єкт злочину — будь-яка особа (фізична, осудна, яка досягла 16-річного віку і не має права доступу до інформації, що обробляється в ЕОМ, АС, комп 'ютерних мережах чи мережах електрозв'язку).

У частині 2 ст. 361 КК встановлена кримінальна відповідальність за ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду. Повторність вчинення злочину — див. ст. 32 КК. Вчинення злочину за попередньою змовою групою осіб — див. ст. 28 КК. При встановленні заподіяної шкоди як значної унаслідок несанкціонованого втручання в роботу ЕОМ, АС, комп 'ютерних мереж чи мереж електрозв'язку слід ураховувати: вар-тість комп'ютерної інформації чи її носіїв, знищених, втрачених чи підроблених; збитки, спричинені неможливістю використання втраче-ної або підробленої чи заблокованої комп'ютерної інформації чи її носіїв; витрати на відновлення змісту підробленої або втраченої комп'ютерної інформації чи її носіїв; збитки внаслідок незаконного використання неправомірно одержаної чи скопійованої комп'ютерної інформації; збитки внаслідок використання підробленої

інформації та ін. У випадках, коли шкода полягає у заподіянні матеріальних збитків, значною вона вважається, згідно з приміткою до ст. 361 КК, якщо вона у сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп 'ютерів), систем і комп'ютерних мереж може іноді висту-пати як спосіб вчинення 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 вико-ристання відомостей, що становлять комерційну таємницю (ст. 231 КК) та ін. У подібних випадках вчинене підлягає кваліфікації за сукупніс-тю: за ст. 361 КК і статтею, що передбачає відповідальність за конкрет-ний злочин, способом здійснення якого було несанкціоноване втручан-ня в роботу електронно-обчислювальних машин (комп'ютерів), систем комп 'ютерних мереж і мереж електрозв'язку.

Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсю дження або збут (ст. 361[1] КК).

Предмет злочину — шкідливі програм-ні та технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп 'ютерів), автоматизованих систем, комп'ютерних мереж та мереж електрозв' язку.

Програмні засоби (комп'ютерні програми) — це певний набір ін-струкцій у вигляді слів, цифр, кодів, схем, символів, виражених у формі, придатній для зчитування комп' ютером, який приводить цю програму в дію для досягнення певної мети. Як предмет цього зло-чину комп'ютерні програми (програмні засоби) повинні бути шкідли-вими, тобто здатними забезпечити несанкціонований доступ до інфор-мації, а також змінити, знищити, пошкодити, заблокувати інформацію комп 'ютерну чи ту, яка передається мережами електрозв'язку. Різно-видом шкідливих комп'ютерних програм є комп'ютерні віруси. Програма-вірус — це спеціально створена програма, яка здатна сама приєднуватись до інших програм (тобто пристосовуватись і «заражати» їх) і при запуску спричиняти різні негативні наслідки: зіпсування фай-лів і каталогів, перекручування інформації, у тому числі результатів обчислення, засмічення чи спотворення пам'яті ЕОМ, створювати інші перешкоди у роботі ЕОМ чи АС.

Шкідливі технічні засоби — це різного роду прилади, обладнання, устаткування тощо, з допомогою яких вчинюється несанкціонований до-ступ до ЕОМ чи АС. Причому ці засоби здатні призвести до витоку, втра-ти (знищення), підробки (фальсифікації), блокування інформації, спотво-рення процесу обробки інформації, що функціонує в ЕОМ, автоматизо-ваних системах, комп 'ютерних системах чи мережах електрозв'язку, або до порушення встановленого порядку її маршрутизації (ст. 361 КК).

Обов'язковою ознакою предметів розглядуваного злочину є те, що своїм призначенням вони мають несанкціоноване втручання в роботу електронно-обчислювальних машин (комп 'ютерів), автоматизованих систем, комп 'ютерних мереж чи мереж електрозв'язку. Відсутність цієї ознаки виключає можливість визнати вказані програмні чи технічні засоби як предмет злочину, передбаченого ст. 361^1 КК.

Об 'єктивна сторона злочину характеризується певними альтерна-тивними діями: 1) створення шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку; 2) розповсюджен-ня таких програмних чи технічних засобів; 3) збут вказаних програм-них чи технічних засобів.

Створення вказаних програмних чи технічних засобів — це виго-товлення програмних чи технічних засобів, внаслідок чого виникають нові шкідливі предмети (яких раніше не існувало), здатні для несанк-ціонованого втручання в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку. До створення таких предметів слід віднести і модифікацію (перероблення) програмних чи технічних засобів, які звичайно використовуються в роботі ЕОМ, АС, у комп 'ютерних мере-жах чи мережах електрозв'язку, а внаслідок перероблення набувають якості шкідливих і здатних до несанкціонованого втручання в ЕОМ, АС, комп'ютерні мережі чи мережі електрозв'язку. Розповсюдження шкідливих програмних чи технічних засобів — це оплатна чи безоплат-на передача у будь-який спосіб зазначених засобів відносно широкому і невизначеному колу осіб (фізичних чи юридичних), навіть через систему Інтернет. Збут шкідливих програмних чи технічних засобів полягає в оплатній (як правило) чи безоплатній (наприклад, подарунок) передачі вказаних засобів іншій, будь-якій особі.

Даний злочин (ч. 1 ст. 361^1 КК) є злочином з формальним складом і для наявності його об'єктивної сторони не потрібно встановлювати настання суспільно небезпечних наслідків.

Суб'єктивна сторона характеризується прямим умислом. При створенні шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп 'ютерів), автоматизованих систем чи комп'ютерних ме-реж, необхідно встановити як обов'язкову ознаку, вказану в диспозиції ст. 361^1 КК, спеціальну мету — використання, розповсюдження або збут цих шкідливих програмних чи технічних засобів (поняття «роз-повсюдження» і «збут» розкриті раніше). Використання шкідливих програмних чи технічних засобів як мета злочину означає, що при створенні зазначених засобів особа має на меті застосовувати ці шкідливі предмети за їх призначенням, тобто для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп 'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

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

У частині 2 ст. 361^1 КК встановлено кримінальну відповідальність за ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду (поняття «значна шкода» — див. примітку до ст. 361 КК).

Несанкціоновані збут або розповсюдження інформації з обме женим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^2 КК). Безпосередній об 'єкт — нормальне (безпечне) функціонування комп'ютерної інфор-мації з обмеженим доступом.

Предмет злочину — інформація з обмеженим доступом, яка збері-гається в електронно-обчислювальних машинах (комп 'ютерах), авто-матизованих системах, комп 'ютерних мережах або носіях такої інфор-мації, створена та захищена відповідно до чинного законодавства.

Комп'ютерна інформація (див. § 1 цього розділу) з обмеженим до-ступом, згідно зі ст. 30

Закону України «Про інформацію», за своїм правовим режимом поділяється на конфіденційну і таємну.

Конфіденційна інформація містить відомості, які перебувають у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і може поширюватися лише за їх бажанням і згодою до встановлених умов і має відповідний правовий статус. Режим до-ступу до конфіденційної інформації громадян та юридичних осіб ви-значають самостійно та встановлюють для неї систему способів за-хисту компетентні державні органи або власники інформації.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу, передбачену законом таємницю, роз-голошення якої завдає шкоди особі, суспільству або державі. Перелік відомостей, що становлять державну таємницю, визначається Законом України «Про державну таємницю» у редакції від 21 вересня 1999 р.[1]

До іншої, передбаченої законом таємниці належить комерційна, банківська, лікарська таємниці, таємниця листування та ін. Правовий режим цих видів таємниць (інформації) регламентується спеціальними законами. Проте вказані види інформації виступають також і як пред-мети інших (самостійних) злочинів. Так, кримінальна відповідальність за збут або розповсюдження вказаних видів інформації передбачена статтями 145, 121, 232, 328 та ін. (за умов відсутності ознаки злочинів проти основ національної безпеки України). Але якщо така інформація, що зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях інформації, несанкціоновано здобувається або розповсюджується, — все вчинене має кваліфікува-тися за сукупністю злочинів — за ст. 361^2 і відповідною статтею КК, яка встановлює відповідальність за збут чи розповсюдження конкрет-ного виду інформації з обмеженим доступом (таємниці).

Інформація з обмеженим доступом як предмет злочину має збері-гатися в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах. Інформація, яка зберігається в мережах електрозв'язку, до предмета даного злочину не належить.

Ознакою комп' ютерної інформації з обмеженим доступом є те, що вона повинна бути створена та захищена відповідно до чинного зако-нодавства. При цьому в кожному випадку для з'ясування наявності цієї ознаки слід звернутися до відповідних законів чи

підзаконних нормативно-правових актів, у яких регламентується порядок створен-ня і захисту такої інформації.

Зміст поняття «носії комп'ютерної інформації» — див. § 1 цього розділу.

Об'єктивна сторона злочину полягає у вчиненні несанкціоновано-го збуту або розповсюдженні комп 'ютерної інформації з обмеженим доступом, яка зберігається в ЕОМ (комп 'ютерах), АС, комп'ютерних мережах або на носіях такої інформації (ст. 361 КК).

Несанкціонований збут інформації з обмеженим доступом, яка зберігається в ЕОМ (комп 'ютерах), АС, комп'ютерних мережах або на носіях такої інформації, — це несанкціоноване розповсюдження такої інформації без згоди її власника на платній основі — шляхом купівлі- продажу, міни та ін.

Несанкціоноване розповсюдження інформації з обмеженим до-ступом, яка зберігається в ЕОМ (комп'ютерах), АС, комп'ютерних мережах або на носіях такої інформації, — це вчинення будь-яких дій, якими без згоди власника інформації така інформація безпосередньо чи опосередковано надається іншим особам чи доводиться до їх відома, вводиться в обіг шляхом будь-якої, крім оплатної, форми. Тут має місце «передача права володіння» такої інформації іншим особам, а так само розголошення інформації.

Розглядуваний злочин (ч. 1 ст. 361^2 КК) є з формальним складом і тому вважається закінченим з моменту вчинення суспільно небезпеч-них дій, зазначених у законі.

Суб'єктивна сторона характеризується виною у формі прямого умислу.

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

У частині 2 ст. 361^2 КК встановлена кримінальна відповідальність за ті самі дії, вчинені

повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду (ст. 361 КК).

Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автомати зованих системах, комп'ютерних мережах або зберігається на но сіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК). Безпосередній об'єкт злочину — нормальне функціону-вання електронно-обчислювальних машин (комп 'ютерів), автоматизо-ваних систем чи комп 'ютерних мереж, комп 'ютерної інформації.

Предмет злочину — інформація, яка оброблюється в електронно- обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах (зміст поняття «комп'ютерна інформація» див. у § 1 цього розділу).

Ознакою предмета цього злочину є те, що ця інформація обробля-ється в електронно-обчислювальних машинах (комп 'ютерах), авто-матизованих системах чи комп' ютерних мережах. Оброблювання ін-формації — це виконання певних дій з допомогою електронно- обчислювальних машин (комп 'ютерів), автоматизованих систем чи комп'ютерних мереж, які включають у себе різні види маніпуляцій з такою інформацією згідно з відповідними комп' ютерними програмами, інструкціями, завданнями, технічними можливостями ЕОМ і т. ін. По-няття оброблення комп 'ютерної інформації включає в себе і зберіган-ня такої інформації.

Предметом цього злочину також є і інформація, яка зберігається на носіях цієї інформації (зміст поняття «електронні носії комп'ютерної інформації» див. у § 1 цього розділу).

Об 'єктивна сторона злочину полягає у несанкціонованій зміні, знищенні або блокуванні комп'ютерної інформації. Обов'язковими ознаками зміни, знищення або блокування комп 'ютерної інформації є те, що ці дії є несанкціонованими, тобто на вчинення таких дій особа, яка має доступ до цієї інформації, не має ні дійсного, ні передбачува-ного права.

Зміна інформації полягає у будь-якій модифікації інформації, що призводить до її перекручення, хоча при цьому інформація в цілому зберігається. До зміни інформації слід віднести і її доповнення іншими, фальсифікованими даними. Причому йдеться про модифікацію змісту інформації. Тому не можна розглядати як ознаку даного злочину зміни, які ЕОМ здійснює автоматично, наприклад, фіксація часу і факту ко-ристування ЕОМ, активізація (використання) певних файлів тощо.

Знищення інформації — це такий вплив на комп'ютерну інформа-цію, внаслідок якого власник позбавляється цієї інформації, тобто втрачає її повністю (ст. 361 КК).

Блокування інформації — див. ст. 361 КК.

Суб'єктивна сторона — умисна форма вини. Мотив і мета значен-ня для кваліфікації не мають, але якщо при цьому переслідується мета вчинення іншого злочину, то такі дії підлягають кваліфікації за сукуп-ністю злочинів.

Суб'єкт злочину — спеціальний: ним може бути особа осудна, фі-зична, яка досягла 16-річного віку і має право (на підставі трудових правовідносин чи договору, або інших юридичних підстав) доступу до комп 'ютерної інформації або носіїв такої інформації, має право експлу-атувати, використовувати за дорученням (і в межах доручення) власни-ка ЕОМ, АС, комп 'ютерні мережі чи носії комп 'ютерної інформації.

У частині 2 ст. 362 КК встановлена кримінальна відповідальність за перехоплення або копіювання інформації, яка оброблюється в ЕОМ (комп'ютерах), АС чи комп'ютерних мережах або зберігається на но-сіях такої інформації, якщо це призвело до її витоку, вчинене особою, яка має право доступу до такої інформації.

Об'єктивну сторону цього злочину становлять дії, які полягають у несанкціонованому перехопленні або копіюванні інформації. Пере-хоплення інформації — це протиправне заволодіння комп 'ютерною інформацією, яка функціонує в ЕОМ (комп ' ютерах), АС чи комп 'ютерних мережах. Ці дії можуть полягати у простому ознайом-ленні з інформацією, блокуванні такої інформації, затриманні переда-чі і її ненадходженні до адресата

протягом певного часу та ін. Копію-вання інформації — це її відтворення в електронному вигляді, перене-сення на інші носії інформації, наприклад, шляхом сканування-випромінювання монітора, спеціальними технічними засобами. При копіюванні комп' ютерної інформації завжди має місце відтворення ін-формації на певних носіях (створення копії) суб'єкта злочину, причому інформація як така залишається непорушеною, у розпорядженні влас-ника (користувача). Копії ж такої інформації отримує суб'єкт злочину.

Перехоплення або копіювання комп'ютерної інформації повинно бути несанкціонованим, тобто незаконним, коли особа на вчинення вказаних дій не має ні дійсного, ні передбачуваного права.

Обов'язковою ознакою цього злочину (ч. 2 ст. 362 КК) є те, що внаслідок несанкціонованого перехоплення або копіювання інформації, яка оброблюється в ЕОМ (комп 'ютерах), АС чи комп'ютерних мережах; та яка зберігається на носіях такої інформації, має місце витік комп 'ютерної інформації як обов'язковий наслідок цього злочину (зміст поняття «витік інформації» див. ст. 361 КК).

Суб 'єктивна сторона, суб'єкт злочину тотожні за ознаками складу злочину, передбаченого ч. 1 ст. 362 КК.

У частині 3 ст. 362 КК встановлена кримінальна відповідальність за дії, вказані в частині 1 або 2 цієї статті, які вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду (ст. 361 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 (ст. 363 КК).
Безпосередній об'єкт — нормальне функціонування ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку.

Предмет злочину — ЕОМ (комп'ютери), АС, комп'ютерні мережі, мережі електрозв'язку, комп'ютерна інформація, а також інформація, що передається мережами електрозв'язку (див. ст. 361 КК).

Об'єктивна сторона характеризується певними обов' язковими ознаками: а) суспільно небезпечними діяннями (діями чи бездіяльніс-тю) у формі: порушення правил експлуатації ЕОМ (комп'ютерів), АС, комп 'ютерних мереж чи мереж електрозв'язку або порушення поряд-ку чи правил захисту інформації, яка в них оброблюється; б) суспільно небезпечними наслідками у вигляді значної шкоди, яка спричиняється вказаними діями; в) причинним зв'язком між суспільно небезпечними діяннями та суспільно небезпечними наслідками.

Стаття 363 КК має бланкетну диспозицію. Отже, при встановленні правил, які порушуються суб'єктом злочину, слід звернутись до відпо-відних законів чи підзаконних актів, у яких встановлюються правила експлуатації ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку, порядок і правила захисту інформації, яка обробляється у вказаних електронних і електротехнічних системах.

Порушення правил експлуатації ЕОМ (комп ' ютерів), АС, комп 'ютерних мереж чи мереж електрозв'язку може виражатися у не-виконанні або неналежному виконанні уповноваженою особою обов'язків із виконання правил експлуатації вказаних ЕОМ та мереж електрозв'язку. Ці порушення можуть виражатися у порушенні як правил апаратного забезпечення, так і правил експлуатації їх програм-ного забезпечення.

Порушення порядку чи правил захисту інформації, яка обробля-ється ЕОМ (комп 'ютерами), АС, комп 'ютерними мережами чи мере-жами електрозв'язку, — це невиконання або неналежне виконання встановлених нормативно-правовими актами вимог (організаційних чи технічних) захисту інформації, що обробляється у вказаних електрон-них системах особами, які мають здійснювати відповідні заходи по забезпеченню захисту інформації. Основними методами та видами технічного захисту комп'ютерної інформації є використання належних технічних засобів захисту, регламентація роботи користувачів про-грамних засобів, елементів і баз даних, носіїв інформації, пошук, ви-явлення та блокування контролюючих додаткових пристроїв, приладів та ін., які надають можливості викрадати, копіювати інформацію чи знищувати її та ін.

Суспільно небезпечними наслідками порушення правил експлуа-тації ЕОМ (комп 'ютерів), АС, комп' ютерних мереж чи мереж електрозв'язку, а також порушення порядку чи правил захисту інфор-мації, яка в них обробляється, можуть бути: витік (в тому числі ви-крадання, копіювання, втрата повна чи часткова інформації), модифі-кування, блокування інформації, підробка, а також порушення вста-новленого порядку її маршрутизації та ін. Ознакою цих наслідків є те, що вказані дії повинні заподіяти значну шкоду власнику інформації (поняття «значна шкода» див. у ст. 361 КК).

Між діями (в альтернативі), що утворюють об'єктивну сторону розглядуваного злочину, і суспільно небезпечними наслідками слід встановлювати необхідний причинний зв'язок.

Суб 'єктивна сторона злочину характеризується умисною чи не-обережною формою вини до порушення правил експлуатації ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку або порядку чи захисту інформації і необережною формою вини до суспільно небезпечних наслідків — значної шкоди, яка спричинена власнику інформації.

Суб 'єкт злочину — особа фізична, осудна, яка досягла 16-річного віку і відповідає за експлуатацію ЕОМ, АС, комп 'ютерних мереж чи мереж електрозв'язку або повинна забезпечувати правила захисту ін-формації, яка в них обробляється (спеціальний суб'єкт).

Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363[1] КК). Безпосередній об'єкт — нормальне функ-ціонування електронно-обчислювальних машин (комп'ютерів), автомати-зованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Предмет злочину — ЕОМ (комп'ютери), АС, комп'ютерні мережі чи мережі електрозв'язку, комп 'ютерна інформація, а також інформація, що передається засобами електрозв'язку.

Об'єктивна сторона характеризується: а) суспільно небезпечними діями у вигляді масового розповсюдження повідомлень електрозв'язку, здійсненого без попередньої згоди адресатів; б) суспільно небезпечни-ми наслідками у вигляді порушення або припинення роботи автомати-зованих систем, комп'ютерних мереж чи мереж електрозв'язку; в) причинним зв'язком зазначених дій із наслідками.

Масове розповсюдження повідомлень електрозв'язку — це надан-ня значній кількості адресатів (досить широкому невизначеному колу осіб) без їх попередньої згоди як однакових, так і різних за змістом повідомлень. Передавання одного чи більше повідомлень одному адресатові або чітко визначеній їх кількості не може розглядатися як масове розповсюдження і не може становити складу цього злочину.

Повідомлення електрозв'язку — це певна інформація (відомості), що сповіщаються комусь і передаються мережами електрозв'язку. У цих повідомленнях можуть міститися судження, які підтверджують певні факти або їх відкидають. Сигнали електрозв'язку, які не містять якихось відомостей, не охоплюються даним поняттям.

При вчиненні цього злочину повідомлення електрозв'язку розповсю-джуються через систему ЕОМ (комп 'ютери), АС, комп'ютерні мережі чи мережі електрозв'язку, в тому числі і через систему Інтернет. Як правило, це зайві для адресата, незапитувані ним і небажані для нього нав'язливі електронні повідомлення рекламного, інформаційно-політичного або комерційного характеру. Ця інформація (відомості) стосується конкретних осіб, організацій, політичних діячів, окремих партій тощо.

Отримання адресатами повідомлень електрозв'язку (навіть коли воно має масовий характер) за їх попередньою згодою не містить скла-ду злочину.

Суспільно небезпечними наслідками цього злочину є порушення або припинення роботи ЕОМ (комп 'ютерів), АС, комп 'ютерних мереж чи мереж електрозв'язку. Порушення роботи ЕОМ (комп 'ютерів), АС, комп' ютерних систем чи систем електрозв' язку — це порушення повне чи часткове процесу функціонування вказаних ЕОМ або повна чи часткова втрата контролю над ними. Унаслідок порушення роботи мережі електрозв' язку втрачається також і здатність забезпечувати за-хист інформації, що передається нею, від знищення, перекручення, блокування, несанкціонованого витоку або від порушення встановле-ного порядку маршрутизації.

Припинення роботи ЕОМ (комп'ютерів), АС чи комп'ютерних мереж має місце у випадках, коли вони взагалі перестають працювати і не можуть виконувати операції по збереженню, введенню, записуван-ню, фіксуванню, перетворенню, зчитуванню, знищенню, реєстрації інформації та ін.

Припинення роботи мережі електрозв'язку — це припинення ви-конання мережами електрозв'язку функцій з передавання або при-йняття знаків, сигналів, письмового тексту, зображень та звуків або інших повідомлень по радіо-, проводових, оптичних або інших елек-тромагнітних системах.

Між суспільно небезпечними діями і суспільно небезпечними на-слідками необхідно встановити причинний зв'язок.

Суб'єктивна сторона — умисна форма вини, мотиви і цілі для кваліфікації злочину значення не мають.

Суб 'єкт злочину — будь-яка фізична особа, що досягла 16-річного віку.

У частині 2 ст. 361 КК встановлена кримінальна відповідальність за ті самі дії, які вчинені повторно або за попередньою змовою групою осіб. При цьому для наявності вказаних кваліфікованих ознак складу цього злочину слід обов'язково встановити, що такими діями завдано значної шкоди.

Контрольні запитання

1. Які злочини передбачені розділом ХУІ КК України? Дайте визначення об'єкта цих злочинів.

2. Якими є предмети злочинів, передбачених розділом ХУІ? Сформулюйте поняття цих предметів.

3. Які об'єктивні та суб'єктивні ознаки притаманні таким зло-чинам:

а) несанкціоноване втручання в роботу електронно - обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

б) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;

в) 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 інфор-мації;

г) несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), авто-матизованих системах, комп'ютерних мережах або зберіга-ється на носіях такої інформації, вчинені особою, яка має право доступу до неї;

д) порушення правил експлуатації електронно-обчислю-вальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється;

е) перешкоджання роботі електронно-обчислювальних ма-шин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв' язку шляхом масового розпо-всюдження повідомлень електрозв' язку.