ТЕМА 15. КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

План:

1. Загальна характеристика кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.
2. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України).
3. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361^1 КК України).
4. 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 (ст. 361^2 КК України).
5. 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 (ст. 362 КК України).
6. 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 України).
7. 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 України).

1. Загальна характеристика кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку згруповані у XVI розділі КК України.

Родовий об'єкт – інформаційна безпека.

Предмет:

1) *інформаційна (автоматизована) система* – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням

технічних і програмних засобів (ст. 1 Закону України «Про захист інформації в інформаційно-комунікаційних системах»);

2) *електронні комунікаційні системи* – визначення в законодавстві немає. Є тільки е.к. мережа;

3) *інформаційно-комунікаційна система* – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле (ст. 1 Закону України «Про захист інформації в інформаційно-комунікаційних системах»);

4) *електронна комунікаційна мережа* – комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг (п. 26 ст. 2 Закону України «Про електронні комунікації»);

5) *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;

6) *автоматизовані системи* (АС) – системи, що здійснюють автоматизовану обробку даних, до складу яких входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення. До складу АС входить принаймні одна ЕОМ (комп'ютер) та периферійні пристрої, що працюють на основі такої ЕОМ: принтер, сканер, модем, мережевий адаптер тощо; АС включають у себе комп'ютерні мережі і мережі електрозв'язку;

7) *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 загальномережевих ресурсів. Комп'ютерні мережі передбачають спільне використання ресурсів обчислювальних центрів (ОЦ), запуск загальних програм, що входять до комп'ютерних систем; ЕОМ можуть включати дві чи більше автоматизованих комп'ютерних системи (АКС) як 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;

8) *мережі електрозв'язку* – це сукупність технічних засобів та споруд зв'язку, з'єднаних у єдиний технологічний процес забезпечення інформаційного обміну – маршрутизації, 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, 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 й обміну інформацією;

9) *комп'ютерна інформація* – це текстова, цифрова, графічна чи інша інформація (дані, відомості) про осіб, предмети, події, явища, що існує в електронному вигляді і знаходиться в ЕОМ, АС чи в комп'ютерній мережі, а також зберігається на відповідних електронних носіях, до яких належать гнучкі магнітні диски (дискети), 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);

10) *інформація, що передається мережами електрозв'язку (телекомунікаційними мережами)* – будь-які відомості, подані у вигляді сигналів, знаків, звуків, зображень чи в інший спосіб (телефонні повідомлення, радіо- та телепередачі тощо), у тому числі й за допомогою комп'ютера, якщо вона передається через мережі електрозв'язку.

Об'єктивна сторона цих кр. пр. може виражатися в *активних діях* (несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж) – ст. 361 КК України – або у кримінально протиправній *бездіяльності* (наприклад, 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 України).

Для об'єктивної сторони деяких кр. пр. потрібно не тільки вчинення суспільно небезпечного діяння (умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів), а й настання суспільно небезпечних наслідків – *матеріальні склади* кр. пр.: порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ч. 1 ст. 363^1 КК України). В інших випадках розглядувані кр. пр. сформульовані як склади із *формальним складом* (Створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ч. 1 ст. 361^1 КК України).

Суб'єкт кр. пр. – особа фізична, осудна, яка досягла *16-річного віку*. У деяких випадках суб'єкт *спеціальний* – особа, яка відповідає за експлуатацію ЕОМ (комп'ютерів), АС, комп'ютерних мереж, мереж електрозв'язку або повинна забезпечувати порядок чи виконання правил захисту інформації, яка в них обробляється (ст. 363 КК України).

Суб'єктивна сторона цих кр. пр. передбачає, як правило, *умисну вину*. Можлива і *необережність* – 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 України).

Мотиви та мета можуть бути різними – помста, прагнення до заволодіння інформацією. Якщо ж викрадення інформації вчиняється з корисливих мотивів і містить ознаки шахрайства, вчинене слід кваліфікувати за сукупністю кр. пр. – за ст.ст. 362 і 190 КК України.

2. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України)

Об'єктивна сторона кр. пр., що розглядається, характеризується: дією у вигляді несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Несанкціоноване втручання в інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж – це самочинне, без дозволу власника або уповноваженої особи проникнення у вказані електронні системи чи мережі. При несанкціонованому втручанні особа протиправно отримує доступ до інформації, що зберігається в системах та мережах, на що вона не має ні дійсного, ні передбачуваного права. Системи чи мережі не належать винному ні на праві власності, ні на будь-якій іншій законній підставі (наприклад, на умовах оренди). Тут завжди має місце злам і проникнення (вторгнення) у систему або мережу. При втручанні в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж завжди має місце негативний вплив на нормальне функціонування цих систем і мереж, а також інформаційних процесів, що в них проходять. Ці дії суперечать 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 захисті, шляхом автоматичного перебирання абонентських номерів («угадування коду»), дії «хакерів», з'єднання з тим чи іншим комп'ютером, підключеним до мережі, використання чужого імені (пароля) за допомогою існуючої помилки в логіці побудови програми тощо, і не впливають на встановлення складу кр. пр. (ст. 361 КК України) як підстави кримінальної відповідальності. Але вони враховуються при оцінці суспільної небезпеки вчинення кр. пр. і призначенні покарання.

Склад цього кр. пр. – *формальний*.

Суб'єкт кр. пр. – будь-яка особа (фізична, осудна, яка досягла *16-річного віку і не має права доступу до інформації*, що обробляється в інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мережах).

Суб'єктивна сторона кр. пр. характеризується *умисною формою вини*. *Мотив і мета* – різні і для кваліфікації значення не мають.

Кваліфікуючі та ***особливо кваліфікуючі ознаки:***

1) повторність (ч. 2 ст. 361 КК України);

2) за попередньою змовою групою осіб(ч. 2 ст. 361 КК України);

3) якщо вказані дії призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до 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, унаслідок ознайомлення з її змістом, шляхом копіювання інформації тощо. При цьому власник не позбавляється інформації, яка йому належить.

Втрата інформації – це припинення існування інформації відносно осіб, які мають право власності на неї. Втрата інформації може бути результатом її знищення, «викрадання», внаслідок якого власник позбавляється належної йому інформації.

Підробка інформації – це дії, що призводять до перекручення (модифікації) змісту інформації, яка обробляється у відповідних системах і мережах, або створення інформації, що за змістом не відповідає дійсності (фальсифікація інформації).

Блокування інформації має місце у випадках, коли внаслідок несанкціонованого втручання в роботу відповідних систем та мереж власник чи уповноважена 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 послідовності оброблення інформації, порядок якої встановлюється власником системи чи мережі. Тут може порушуватись порядок: збирання, ведення, записування, перетворення, зчитування, знищення, реєстрації, прийняття, отримання, передавання інформації. Унаслідок вказаного спотворення процесу обробки інформації одержується інший результат, ніж очікувався.

Порушення встановленого порядку маршрутизації – це протиправна, внаслідок несанкціонованого втручання, зміна адресата інформації, яка передається електронними комунікаційними каналами. Унаслідок порушення порядку маршрутизації адресат не отримує інформації, яка була для нього направлена, або таку інформацію отримують і інші особи, яким ця інформація не була адресована.

4) значна шкода (ч. 4 ст. 361 КК України). Відповідно до примітки до ст. 361 України значною шкодою у ст.ст. 361-363-1 вважається така шкода, яка в триста і більше разів перевищує неоподатковуваний мінімум доходів громадян.

5) такі дії створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків (ч. 4 ст. 361 КК України);

6) дії, передбачені частиною третьою або четвертою цієї статті, вчинені під час дії воєнного стану (ч. 5 ст. 361 КК України)

Дії, передбачені ч. 1-4 цієї статті, не вважаються несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж.

Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж може іноді виступати як спосіб вчинення інших кр. пр., наприклад: диверсії (ст. 113 КК України), шпигунства (ст. 114 КК України), шахрайства (ст. 190 КК України), незаконних дій з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення (ст. 200 КК України), незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231 КК України) та ін. У подібних випадках вчинене підлягає кваліфікації за сукупністю: за ст. 361 КК України і статтею, що передбачає відповідальність за конкретне кр. пр., способом здійснення якого було несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

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

Предмет кр. пр. – шкідливі програмні та технічні засоби, призначені для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Програмні засоби (комп'ютерні програми) – це певний набір інструкцій 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 кр. пр. комп'ютерні програми (програмні засоби) повинні бути ***шкідливими,*** тобто здатними забезпечити несанкціонований доступ до інформації, а також змінити, знищити, пошкодити, заблокувати інформацію, яка передається мережами чи є у системі. Різновидом 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 файлів і каталогів, перекручування інформації, у тому числі результатів обчислення, засмічення чи спотворення пам'яті ЕОМ (комп'ютерів), створювати інші перешкоди у роботі систем чи мереж.

Шкідливі технічні засоби – це різного роду прилади, обладнання, устаткування тощо, з допомогою яких вчинюється несанкціонований доступ до ЕОМ (комп'ютерів) чи АС. Причому ці засоби здатні призвести до витоку, втрати (знищення), підробки (фальсифікації), блокування інформації, спотворення процесу обробки інформації, що функціонує інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, або до порушення встановленого порядку її маршрутизації.

Обов'язковою ознакою предметів розглядуваного кр. пр. є те, що своїм призначенням вони мають несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Відсутність цієї ознаки виключає можливість визнати вказані програмні чи технічні засоби як предмет кр. пр., передбаченого ст. 361[1] КК України.

Об'єктивна сторона кр. пр. характеризується певними альтернативними діями:

1) створення шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку;

2) розповсюдження таких програмних чи технічних засобів;

3) збут вказаних програмних чи технічних засобів.

Створення вказаних програмних чи технічних засобів – це виготовлення програмних чи технічних засобів, внаслідок чого виникають нові шкідливі предмети (яких раніше не існувало), здатні для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. До створення таких предметів слід віднести і ***модифікацію*** (перероблення) програмних чи технічних засобів, які звичайно використовуються в роботі інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, а внаслідок перероблення набувають якості шкідливих і здатних до несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Розповсюдження шкідливих програмних чи технічних засобів – це оплатна чи безоплатна 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 будь-якій іншій особі.

Це кр. пр. (ч. 1 ст. 361[1] КК України) із *формальним складом* і для наявності його об'єктивної сторони непотрібно встановлювати настання суспільно небезпечних наслідків.

Суб'єкт кр. пр. – фізична, осудна особа, яка досягла *16-річного віку*.

Суб'єктивна сторона характеризується *прямим умислом*. При створенні шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, необхідно встановити як обов'язкову ознаку, вказану в диспозиції ст. 361[1] КК України, ***спеціальну мету*** – використання, розповсюдження або збут цих шкідливих програмних чи технічних засобів. Використання шкідливих програмних чи технічних засобів як мета кр. пр. означає, що при створенні зазначених засобів особа має на меті застосовувати ці шкідливі предмети за їх призначенням, тобто для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Кваліфікуючі ознаки (ч. 2 ст. 361[1] КК України):

1) повторність;
2) за попередньою змовою групою осіб;
3) заподіяння значної шкоди.

4. 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 (ст. 361[2] КК України)

Предмет кр.пр. – інформація з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), АС, комп'ютерних мережах або носіях такої інформації, створена та захищена відповідно до чинного законодавства.

Комп'ютерна інформація з обмеженим доступом, згідно зі ст. 21 Закону України «Про інформацію», за своїм правовим режимом поділяється на конфіденційну, таємну та службову.

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 та має відповідний правовий статус. Режим доступу до конфіденційної інформації громадян та юридичних осіб визначають самостійно та встановлюють для неї систему способів захисту компетентні державні органи або власники інформації.

До *таємної інформації* належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству або державі. Перелік відомостей, що

становлять ***державну таємницю,*** визначається Законом України «Про державну таємницю».

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

Інформація з обмеженим доступом як предмет кр. пр. має зберігатися в ЕОМ (комп'ютерах), АС, комп'ютерних мережах. Інформація, яка зберігається в мережах електрозв'язку, до предмета цього кр. пр. не належить.

Ознакою комп'ютерної інформації з обмеженим доступом є те, що вона має бути створена та захищена відповідно до чинного законодавства. При цьому в кожному випадку для з'ясування наявності цієї ознаки слід звернутися до відповідних законів чи підзаконних нормативно-правових актів, в яких регламентується порядок створення й захисту такої інформації.

Об'єктивна сторона кр. пр. полягає у вчиненні несанкціонованого 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. 361^2 КК України).

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 – шляхом купівлі-продажу, міни тощо.

Несанкціоноване розповсюдження інформації з обмеженим доступом, 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.

Розглядуване кр. пр. (ч. 1 ст. 361^2 КК України) є з *формальним складом* і тому вважається *закінченим* з моменту вчинення суспільно небезпечних дій, зазначених у законі.

Суб'єкт кр. пр. – фізична, осудна особа, яка досягла *16-річного віку*.

Суб'єктивна сторона характеризується виною у формі *прямого умислу*.

Кваліфікуючі ознаки (ч. 2 ст. 361^2 КК України):
1) повторність;
2) за попередньою змовою групою осіб;
3) заподіяння значної шкоди.

5. 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 (ст. 362 КК України)

Предмет кр. пр. – інформація, яка оброблюється в ЕОМ (комп'ютерах), АС чи комп'ютерних мережах**.**

Ознакою предмета цього кр. пр. є те, що ця інформація обробляється в ЕОМ (комп'ютерах), АС чи комп'ютерних мережах. *Оброблювання інформації* – це виконання певних дій з допомогою електронно-обчислювальних машин (комп'ютерів), автоматизованих систем чи комп'ютерних мереж, які включають в себе різні види маніпуляцій з такою інформацією згідно з відповідними комп'ютерними програмами, інструкціями, завданнями, технічними можливостями ЕОМ і т. ін. Поняття оброблення комп'ютерної інформації включає в себе і зберігання такої інформації. Предметом цього кр. пр. також є інформація, яка зберігається на носіях цієї інформації**.**

Об'єктивна сторона кр. пр. 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 передбачуваного 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 цього кр. пр. зміни, які ЕОМ здійснює автоматично, наприклад, фіксація часу і факту користування ЕОМ, активізація (використання) певних файлів тощо.

Знищення інформації – це такий вплив на комп'ютерну інформацію, внаслідок якого власник позбавляється цієї інформації, тобто втрачає її повністю.

Суб'єкт кр. пр. – *спеціальний*: ним може бути особа осудна, фізична, 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 експлуатувати, використовувати за дорученням (і в межах доручення) власника ЕОМ (комп'ютери), АС, комп'ютерні мережі чи носії комп'ютерної інформації.

Суб'єктивна сторона – *умисна форма вини*. *Мотив і мета* значення для кваліфікації не мають, але якщо при цьому ставиться за мету вчинення іншого кр. пр., то такі дії підлягають кваліфікації за сукупністю кр. пр.

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

Об'єктивну сторону цього кр. пр. становлять дії, які полягають у несанкціонованому перехопленні або копіюванні інформації. Перехоплення інформації – це протиправне заволодіння комп'ютерною інформацією, яка функціонує в ЕОМ (комп'ютерах), АС чи комп'ютерних мережах. Ці дії можуть полягати у простому ознайомленні з інформацією, блокуванні такої інформації, затриманні передачі і її ненадходженні до адресата протягом певного часу та ін. Копіювання інформації – це її відтворення в електронному вигляді, перенесення на інші носії інформації, наприклад, шляхом сканування-випромінювання монітора, спеціальними технічними засобами. При копіюванні комп'ютерної інформації завжди має місце відтворення інформації на певних носіях (створення копії) суб'єкта кр. пр., причому інформація як гака залишається непорушеною, у розпорядженні власника (користувача). Копії ж такої інформації отримує суб'єкт кр. пр. 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 кр. пр. (ч. 2 ст. 362 КК України) є те, що внаслідок несанкціонованого перехоплення або копіювання інформації, яка оброблюється в ЕОМ, або яка зберігається на носіях такої інформації, має місце ***витік*** комп'ютерної інформації як обов'язковий наслідок цього кр. пр.

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

Кваліфікуючі ознаки (ч. 3 ст. 362 КК України):

1) повторність;
2) за попередньою змовою групою осіб;
3) заподіяння значної шкоди.

6. 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 України)

Предмет кр. пр. – ЕОМ (комп'ютери), АС, комп'ютерні мережі, мережі електрозв'язку, комп'ютерна інформація, а також інформація, що передається мережами електрозв'язку.

Об'єктивна сторона характеризується певними обов'язковими ознаками:

1) суспільно небезпечними діяннями (діями чи бездіяльністю) у формі: порушення правил експлуатації ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку або порушення порядку чи правил захисту інформації, яка в них обробляється;

2) суспільно небезпечними наслідками у вигляді значної шкоди, яка спричиняється вказаними діями;

3) причинним зв'язком між суспільно небезпечними діяннями та суспільно небезпечними наслідками.

Ст. 363 КК України має *бланкетну* диспозицію. Отже, при встановленні правил, які порушуються суб'єктом кр. пр., слід звернутись до відповідних законів чи підзаконних актів, в яких встановлюються правила експлуатації ЕОМ (комп'ютерів), 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 невиконанні 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 програмного забезпечення.

Порушення порядку чи правил захисту інформації, яка обробляється ЕОМ (комп'ютерами), АС, комп'ютерними мережами чи мережами електрозв'язку, – це невиконання або неналежне виконання встановлених нормативно-правовими актами вимог (організаційних чи технічних) захисту інформації, що обробляється у вказаних електронних системах особами, які мають здійснювати відповідні заходи щодо забезпечення захисту інформації. Основними методами та видами технічного захисту комп'ютерної інформації є використання належних технічних засобів захисту, регламентація роботи користувачів програмних засобів, елементів і баз даних, носіїв інформації, пошук, виявлення та блокування контролюючих додаткових пристроїв, приладів тощо, які надають можливість викрадати, копіювати інформацію чи знищувати її тощо.

Суспільно небезпечними наслідками порушення правил експлуатації ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку, а також порушення порядку чи правил захисту інформації, яка в них обробляється, можуть бути: витік (у тому числі викрадання, копіювання, втрата повна чи часткова інформації), модифікування, блокування інформації, підробка, а також порушення встановленого порядку її маршрутизації та ін. Ознакою цих наслідків є те, що вказані дії повинні заподіяти *значну шкоду* власнику інформації.

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

Суб'єкт кр. пр. – особа фізична, осудна, яка досягла *16-річного віку* і *відповідає за експлуатацію* ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку або повинна забезпечувати правила захисту інформації, яка в них обробляється (спеціальний суб'єкт).

Суб'єктивна сторона кр. пр. характеризується у*мисною чи необережною формою вини* до порушення правил експлуатації ЕОМ (комп'ютерів), 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.

7. 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 України)

Безпосередній об'єкт – нормальне функціонування ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку.

Предмет кр. пр. – 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:

1) суспільно небезпечними діями у вигляді масового розповсюдження повідомлень електрозв'язку, здійсненого без попередньої згоди адресатів;

2) суспільно небезпечними наслідками у вигляді порушення або припинення роботи автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

3) причинним зв'язком зазначених дій із наслідками.

Масове розповсюдження повідомлень електрозв'язку – це надання 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 кр. пр.

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 цим поняттям.

При вчиненні цього кр. пр. повідомлення електрозв'язку розповсюджуються через систему ЕОМ (комп'ютери), АС, комп'ютерні мережі чи мережі електрозв'язку, у тому числі й 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 складу кр. пр.

Суспільно небезпечними наслідками цього кр. пр. є порушення або припинення роботи ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку. Порушення роботи ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж 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 здатність забезпечувати захист інформації, що передається нею, від знищення, перекручення, блокування, несанкціонованого витоку або від порушення встановленого 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, записуванню, фіксуванню, перетворенню, зчитуванню, знищенню, реєстрації інформації та ін.

Припинення роботи мережі електрозв'язку – це припинення виконання мережами електрозв'язку функцій з передавання або прийняття знаків, сигналів, письмового тексту, зображень та звуків або інших повідомлень по радіо-, проводових, оптичних або інших електромагнітних системах.

Між суспільно небезпечними діями і суспільно небезпечними наслідками необхідно встановити причинний зв'язок.

Суб'єкт кр. пр. – будь-яка фізична осудна особа, що досягла *16-річного віку*.

Суб'єктивна сторона – *умисна форма вини*, мотиви і цілі для кваліфікації кр. пр. значення не мають.

Кваліфікуючі ознаки (ч. 2 ст. 363^1 КК України):

1) повторність;
2) за попередньою змовою групою осіб.

Питання до самоконтролю:

1. Якими є предмети кримінальних правопорушень, передбачених розділом XVI КК України?
2. Як кваліфікують правопорушення, в яких комп'ютери виступають засобом заволодіння чужим майном?
3. Як кваліфікують розповсюдження за допомогою комп'ютерних мереж і мереж електрозв'язку матеріалів із закликами до вчинення дій з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України?
6. Які об'єктивні, суб'єктивні та кваліфікуючі ознаки кримінального правопорушення, передбаченого ст. 362 КК?

5. Які об’єктивні, суб’єктивні та кваліфікуючі ознаки кримінального правопорушення, передбаченого ст. 361 КК?