**Лекція № 3 Технології захисту інформації**

**План**

1. *Поняття злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж*
2. *Види злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж*
3. *Злочинна діяльність щодо порушення правил експлуатації ЕОМ*

# Поняття злочинів у сфері використання електронно- обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж

Науково-технічний прогрес не можливий без широкомасштабного впровадження в управлінську діяльність, у різні сфери науки, техніки та виробництва електронно-обчислювальної техніки. Це потребує розвитку і вдосконалення правових засобів регулювання суспільних відносин у сфері комп'ютеризації діяльності людини. Регулювання здійснюється такими нормативними актами: Законом України «Про захист інформації в автоматизованих системах» від 5 липня 1994 р., Положення про технічний захист інформації в Україні, затвердженим Указом Президента України від 27 вересня 1999 р. № 1229 та ін.

У XVI розділі КК України встановлена відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. До них відносяться: незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (ст. 361), викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем (ст. 362), порушення правил експлуатації автоматизованих електронно-обчислювальних систем (ст. 363).

*Родовим об'єктом* цих злочинів є суспільні відносини у сфері безпеки комп'ютерної інформації і нормального функціонування електронно- обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж.

*Предмет злочину:* 1) електронно-обчислювальна машина (ЕОМ) — комп'ютер — комплекс технічних засобів, призначених для автоматичної обробки інформації в процесі вирішення обчислювальних та інформаційних задач; 2) автоматизовані комп'ютерні системи (АКС) — сукупність взаємопов'язаних ЕОМ, периферійного обладнання та програмного забезпечення, призначених для автоматизації прийому, зберігання, обробки, пошуку і видачі інформації споживачам. Комп'ютерні системи можуть бути регіонального та галузевого характеру; 3) комп'ютерні мережі (мережа ЕОМ) — це з'єднання декількох комп'ютерів (ЕОМ) та комп'ютерних систем, що взаємопов'язані і розташовані на фіксованій території та орієнтовані на колективне використання загальномережових ресурсів. Комп'ютерні мережі передбачають спільне використання ресурсів обчислювальних центрів (ОЦ), запуск загальних програм, які входять до комп'ютерних систем; 4) носії комп'ютерної інформації — фізичні об'єкти, машинні носії, призначені для постійного зберігання, перенесення і обробки комп'ютерної інформації. До них відносяться гнучкі магнітні диски (дискети), жорсткі магнітні диски

(вінчестери), касетні магнітні стрічки (стримери), магнітні барабани, магнітні карти тощо; 5) комп'ютерна інформація — це текстова, цифрова, графічна чи інша інформація (дані, відомості) про осіб, предмети, події, яка існує в електронному виді, зберігається на відповідних електронних носіях і може використовуватися, оброблятися або змінюватися за допомогою ЕОМ (комп'ютерів).

*Об'єктивна сторона* цих злочинів може виражатися в активних діях (наприклад, в незаконному втручанні в роботу автоматизованих електронно- обчислювальних машин (комп'ютерів), їх систем чи комп'ютерних мереж, в розповсюдженні комп'ютерного вірусу (ст. 361), а також в злочинній бездіяльності, наприклад, при порушенні правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж (ст. 363).

Для об'єктивної сторони цих злочинів потрібне не тільки вчинення суспільне небезпечного діяння (незаконне втручання в роботу ЕОМ, викрадення, привласнення комп'ютерної інформації тощо), а й настання суспільне небезпечних наслідків (перекручення або знищення комп'ютерної інформації чи носіїв такої інформації, заподіяння істотної шкоди власнику ЕОМ (комп'ютерів), систем та комп'ютерних мереж (ч. 2 ст. 361)). При цьому вимагання комп'ютерної інформації може розглядатися і як злочин з формальним (і усіченим) складом.

*Суб'єктивна сторона* цих злочинів передбачає, як правило, умисну вину. Хоч можлива і необережність — при порушенні правил експлуатації автоматизованих електронно-обчислювальних систем (ст. 363).

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

*Суб'єкт* цього злочину — будь-яка особа, а у деяких випадках суб'єкт спеціальний — службова особа (ст. 362), особа, відповідальна за експлуатацію ЕОМ (ст. 363).

# Види злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж

**Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж чи мереж електрозв’язку** (ст. 361). *Об'єктивна сторона* цього злочину виражається в двох формах:

1. *У незаконному втручанні в роботу автоматизованих електронно- обчислювальних машин, їх систем чи комп'ютерних мереж.* Втручання полягає у проникненні до цих машин, їх систем чи мереж і вчиненні дій, які порушують режим роботи ЕОМ, припиняють (частково чи у повному обсязі) їх роботу. 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 будь- якій іншій законній підставі (наприклад на умовах оренди).

Тут завжди має місце злом і проникнення в програму чужого комп'ютера, системи чи мережі ЕОМ. Способи втручання в роботу електронно- обчислювальних машин можуть бути різними: шляхом виявлення слабких місць в захисті, шляхом автоматичного перебору абонентських номерів (

«вгадування коду» — «дії «хакерів»), з'єднання з тим або іншим комп'ютером, підключеним до телефонної мережі, використання чужого імені (пароля) за допомогою використання помилки в логіці побудови програми тощо.

Наслідком цього діяння має бути перекручення або знищення комп'ютерної інформації чи носіїв такої інформації. Перекручення — це зміна змісту або форми інформації, закладеної в носії, коли можливість використання або відновлення цієї інформації або її фрагментів істотно ускладнена. Знищення комп'ютерної інформації полягає в такій її зміні, коли використання чи відновлення комп'ютерної інформації неможливе. Знищення носіїв комп'ютерної інформації полягає в руйнівному впливі на них (механічному, електронному), внаслідок чого вони стають повністю непридатними і не можуть використовуватися за своїм цільовим призначенням (наприклад знищення вінчестера, дискети, стримера тощо).

1. У розповсюдженні комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в ці машини, системи чи комп'ютерні мережі та здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації. Комп'ютерний вірус — це шкідлива програма, яка «інфікує» носії комп'ютерної інформації, вставляючи в них власні копії. Програма, що містить комп'ютерний вірус, володіє реальною і досить високою мірою можливості знищення, блокування, модифікації комп'ютерної інформації, порушення роботи ЕОМ, їх систем чи мереж. Тому розповсюдження комп'ютерного вірусу («злом» комп'ютерних систем і мереж за допомогою «вірусної атаки») становить підвищену небезпеку суспільним відносинам у сфері комп'ютерної безпеки.

Засобами вчинення цього злочину виступають програмні та технічні засоби. Програма-вірус — це спеціально створена програма, здатна мимовільно приєднуватися до інших програм (тобто «заражати» їх) і при запуску виконувати різні небажані дії: псування файлів і каталогів, спотворення результатів обчислення, засмічення або стирання пам'яті, створення перешкод в роботі ЕОМ. Технічні засоби — це електронно-обчислювальні машини (комп'ютери) та їх системи, шляхом яких вірусні програми протиправне вводяться в базу даних ЕОМ (комп'ютерів), їхні системи чи мережі. При цьому вони мають бути призначеними для незаконного проникнення в електронно- обчислювальні машини (комп'ютери), їхні системи чи мережі та здатними спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації.

Злочин вважається закінченим з моменту розповсюдження (введення в базу даних ЕОМ. (комп'ютерів), їх систем чи мереж комп'ютерного вірусу.

*Суб'єктивна сторона* цього злочину — умисел — прямий або непрямий.

*Суб'єкт* цього злочину — будь-яка особа.

У частині 2 ст. 361 встановлена відповідальність за ті самі дії, якщо вони заподіяли істотну шкоду або вчинені повторно чи за попередньою змовою групою осіб.

*Покарання за злочин:* за ч. 1 ст. 361 — штраф до сімдесяти неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до двох років, або обмеження волі на той самий строк; за ч. 2 ст. 361 — обмеження волі на строк до п'яти років або позбавлення волі на строк від трьох до п'яти років.

**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). *Предмет* злочину — комп'ютерна інформація, введена (закладена) в електронно-обчислювальні машини (комп'ютери), їхні системи чи мережі, а також носії такої інформації.

*Об'єктивна сторона* цього злочину передбачає активні дії, які виражаються у викраденні, привласненні, вимаганні комп'ютерної інформації або у заволодінні нею шляхом шахрайства чи зловживання службовою особою своїм службовим становищем. Внаслідок вчинення цих дій власник чи інша особа, яка володіє комп'ютерною інформацією, позбавляються такої інформації, вона вибуває з їх володіння і не може ними використовуватися.

Об'єктивні ознаки викрадення, привласнення, вимагання комп'ютерної інформації, заволодіння нею шляхом шахрайства потрібно трактувати так само, як і в злочинах проти власності — за статтями 185, 186, 189, 190 і 191.

Для наявності об'єктивної сторони слід встановити не тільки вчинення особою одного з діянь, вказаних у ч. 1 ст. 362, але і настання суспільне небезпечних наслідків — власник або інша особа, яка володіє комп'ютерною інформацією, позбавляється її внаслідок протиправних дій особи і вона переходить до володіння особи, що вчинила зазначений злочин. Вимагання комп'ютерної інформації вважається закінченим з моменту отримання вимоги передачі комп'ютерної інформації або передачі права на таку інформацію, поєднану з погрозою (ст. 189).

*Суб'єктивна сторона* цього злочину — вина у формі прямого умислу.

*Суб'єкт* цього злочину — будь-яка особа. У разі заволодіння комп'ютерною інформацією шляхом зловживання службовою особою своїм службовим становищем або шляхом привласнення суб'єкт злочину спеціальний

— службова особа або особа, якій інформація була ввірена чи знаходилася в її віданні.

Якщо при викраденні комп'ютерної інформації до потерпілого було застосоване насильство і заподіяні, наприклад, тілесні ушкодження, все вчинене слід кваліфікувати за сукупністю злочинів — за ст. 362 і відповідною статтею про злочини проти життя та здоров'я особи. Викрадення, привласнення, вимагання комп'ютера, що містить інформацію чи носії комп'ютерної інформації, що є значною майновою цінністю, або заволодіння такими предметами шляхом шахрайства, зловживання службовим становищем або ж шляхом розбою має кваліфікуватися також за сукупністю злочинів: за ст. 362 і за відповідними статтями розділу про злочини проти власності.

У частині 2 ст. 362 передбачена відповідальність за ті самі дії, вчинені повторно або за попередньою змовою групою осіб. У частині 3 ст. 362 встановлена відповідальність за дії, передбачені частинами 1 або 2 цієї статті, якщо вони заподіяли істотну шкоду.

*Покарання за злочин:* за ч. 1 ст. 362 — штраф від п'ятдесяти до двохсот неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до двох років; за ч. 2 ст. 362 — штраф від ста до чотирьохсот неоподатковуваних мінімумів доходів громадян або обмеження волі на строк до трьох років, або позбавлення волі на той самий строк; за ч. З ст. 362 — позбавлення волі на строк від двох до п'яти років.

# Злочинна діяльність щодо порушення правил експлуатації ЕОМ

**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). *Предмет* злочину — автоматизовані електронно- обчислювальні машини (комп'ютери), їх системи **чи комп'ютерні мережі.**

*Об'єктивна сторона* цього злочину виражається у порушенні правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж. Правила експлуатації ЕОМ — це будь-які технічні правила, які регламентують порядок використання таких машин, збереження комп'ютерної інформації, а також забезпечення засобів захисту автоматизованих електронно-обчислювальних машин. Порушення правил може виражатися як в активних діях, коли особа діє всупереч розпорядженням, закріпленим в правилах, так і у формі бездіяльності — невиконання обов'язків з належного використання (обслуговування) ЕОМ.

*Об'єктивна сторона* цього злочину передбачає не тільки вчинення діяння (порушення правил експлуатації ЕОМ), а й настання суспільне небезпечних наслідків у вигляді: викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту, або незаконного копіювання комп'ютерної інформації, або істотного порушення роботи таких машин, їх систем чи комп'ютерних мереж.

Незаконне копіювання комп'ютерної інформації полягає у виготовленні та привласненні копії ( «дубліката») носія інформації (дискети, вінчестера тощо). Причому виготовлення копії завжди має бути незаконним: особа не мала ні дійсного, ні передбачуваного права на такі дії, вони були вчинені без дозволу власника інформації або з порушенням встановленого порядку. Істотне порушення роботи електронно-обчислювальних машин полягає у виході з ладу електронної інформаційної системи чи мережі на значний час, що негативно вплинуло на діяльність організації, установи, підприємства внаслідок втрати комп'ютерної інформації і припинення функціонування комп'ютерних мереж тощо. Істотне порушення ЕОМ — поняття оціночне і в кожному конкретному випадку підлягає уточненню і конкретизації.

Злочин вважається закінченим з моменту настання вказаних наслідків.

*Суб'єктивна сторона* цього злочину. Щодо порушення правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж допустима будь-яка форма вини, як умисел, так і необережність, а щодо суспільне небезпечних наслідків можлива тільки необережна форма вини.

*Суб'єкт* злочину спеціальний — особа, відповідальна за експлуатацію автоматизованих електронно-обчислювальних машин, їх систем чи

комп'ютерних мереж (інженери, наукові співробітники, працівники обслуговуючого персоналу та інші). На цю особу повинні покладатися обов'язки з правильного використання (експлуатації), забезпечення, відповідно до технічних норм ЕОМ, підтримування їх у робочому стані, оновлення і забезпечення збереження інформації тощо.

Якщо зазначені у ст. 353 дії вчинені службовою особою, то за наявності в її діях ознак службових злочинів, передбачених статтею 366 або 365, вчинене слід кваліфікувати за сукупністю злочинів.

У частині 2 ст. 363 передбачена відповідальність за ті самі дії, якщо вони заподіяли істотну шкоду. Йдеться про те, що внаслідок порушення правил експлуатації ЕОМ настають не лише суспільно небезпечні наслідки, вказані у ч. 1 ст. 363, в тому числі й істотне порушення роботи ЕОМ, а й їх власнику заподіюється істотна шкода — матеріальна, майнова, організаційна тощо. Істотна шкода — поняття оціночне.

*Покарання за злочин:* за ч. 1 ст. 363 — штраф до п'ятдесяти неоподатковуваних мінімумів доходів громадян або позбавлення права обіймати певні посади чи займатися певною діяльністю на строк до п'яти років, або виправні роботи на строк до двох років; за ч 2 ст. 363 — штраф до ста неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до двох років, або обмеження волі на строк до п'яти років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.