Гавловський В.Д., Камлик М.І. Законодавчі та інші нормативно-правові акти, спрямовані на боротьбу з організованою злочинністю та корупцією (параграф 5.2. Розділу V. Прогноз і правова база протидії організованій злочинності в Україні) // Організована злочинність в Україні /за ред. Я.Ю. Кондратьєва. - К.: НАВСУ, 1999. С. 94-107.

Гавловський В.Д., Цимбалюк В.С. Організована злочинність та інформаційні технології (параграф 3.5. Розділу III. Основні напрями та тенденції організованої злочинності в Україні) // Організована злочинність в Україні /за ред. Я.Ю. Кондратьєва. - К.: НАВСУ, 1999. С.73-78.

Романюк Б.В. Камлик М.І., Гавловський В.Д., Хахановський В.Г. Цимбалюк В.С. Виявлення та розслідування злочинів, що вчиняються за допомогою комп`ютерних технологій. Посібник /За ред. Я.Ю. Кондратьєва. - К. НАВСУ. 2000. - 64с.

**УДК 681. 3: 34**

# ПРОБЛЕМИ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ВТРУЧАННЯ В РОБОТУ АВТОМАТИЗОВАНИХ СИСТЕМ (ст. 198[1] КК)

***Петро Андрушко***
*Київський Національний університет імені Тараса Шевченка*

*Анотація:* **Стаття присвячена проблемам кримінальної відповідальності за злочин проти нормальної роботи автоматизованих систем, у відповідності із законодавством України**.
*Summary*: **This article is devoted to the problems of the criminol responsibilitu for the commiting crimes against the normal work of the automation systems, acording to the Ukrainian laws.**
*Ключові слова:* **Злочин, автоматизовані системи, інформація, втручання в роботу, перекручення, знищення.**

Втручання у роботу автоматизованих систем (АС) є однією із двох форм вчинення злочину, передбаченого ст. 198[1] КК. Інша форма вчинення цього злочину – це розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручення або знищення інформації чи то носіїв інформації. Зазначимо, що само по собі виготовлення таких програмних і технічних засобів не є злочином, за винятком випадків, коли метою такого виготовлення є їх наступне розповсюдження. У цьому разі дії особи мають кваліфікуватися як готування до вчинення злочину у формі розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручення або знищення інформації чи носіїв інформації. Названі програмні і технічні засоби і є предметом цього злочину.

Під розповсюдженням програмних і технічних засобів, призначених для незаконного проникнення в АС і здатних спричинити перекручення або знищення інформації чи носіїв інформації треба розуміти: 1) їх передачу будь-яким способом і на будь-яких підставах (продаж, дарування, обмін, надання можливості скопіювати тощо) з метою їх використання для несанкціонованого доступу до інформації особами, які згідно з правилами розмежування доступу до інформації, встановленими власником інформації чи уповноваженою ним особою, не мають права доступу до такої інформації; 2) їх "закладку" в АС на стадії її виготовлення, ремонту, реалізації, користування з метою використання в майбутньому для здійснення несанкціонованого доступу до інформації; 3) ознайомлення інших осіб із змістом програмних засобів чи технічними характеристиками або технологією виготовлення та використання програмних і технічних засобів для незаконного проникнення в АС.

Програмні засоби, призначені для незаконного проникнення в АС, — це спеціальні комп'ютерні програми (програмні блоки, програмне забезпечення), з допомогою яких можна здійснити несанкціонований доступ до інформації, яка зберігається чи обробляється в АС, і які здатні спотворити або знищити інформацію (її носії) шляхом спотворення процесу обробки інформації.

Технічні засоби, призначені для незаконного проникнення в АС — це різного роду прилади, обладнання, устаткування тощо, з допомогою яких можливе або безпосереднє підключення до АС чи каналів передачі даних, або які здатні шляхом формування сигналів, полів, середовищ створити умови для несанкціонованого доступу до інформації з метою ознайомлення з такою інформацією особами, які не мають права доступу до неї, або з метою впливу на процес обробки інформації в АС, порушення роботи АС, перекручення або знищення інформації чи її носіїв.

Обов'язковою ознакою (властивістю) програмних і технічних засобів, призначених для незаконного проникнення в АС, для визнання їх предметом коментованого злочину, є їх здатність впливати на процес обробки інформації, його зміну, спотворення, в результаті чого інформація (її носії) може бути знищена чи перекручена, тобто змінена (спотворена). Якщо ж такі засоби за своїми технічними характеристиками не мають такої властивості, їх розповсюдження складу злочину, передбаченого ст. $198^1$, не утворює. Використання таких програмних і технічних засобів, наприклад, для незаконного ознайомлення з інформацією, яка обробляється чи зберігається в АС, може кваліфікуватися за статтями 56, 57 чи $148^6$.

Детальніше зупинимося на першій формі вчинення злочину – умисному втручанні у роботу автоматизованих систем, оскільки, по-перше, такі дії становлять підвищену суспільну небезпеку і, по-друге, за їх допомогою вчинюються, як правило, інші, більш тяжкі злочини: розкрадання державного, колективного чи індивідуального майна громадян; виготовлення, в тому числі підробка, цінних паперів у бездокументарній формі їх існування (статті 79 чи $148^8$ КК); тощо.

Предметом злочину у формі умисного втручання у роботу автоматизованих систем, залежно від мети такого втручання, можуть визнаватись: 1) інформація, яка використовується в АС, — сукупність усіх даних і програм, які використовуються в АС незалежно від засобу їх фізичного та логічного представлення (ст. 1 Закону від 5 липня 1994 р. "Про захист інформації в автоматизованих системах" // Відомості Верховної Ради України. — 1994. — № 31 — Ст. 286); 2) носії інформації — фізичні об'єкти, поля і сигнали, хімічні середовища, нагромаджувачі даних в інформаційних системах (ст. 24 Положення про технічний захист інформації в Україні, затвердженого постановою Кабінету Міністрів України від 9 вересня 1994 р. № 632 // ЗП України. — 1994. — № 12. — Ст. 302); 3) автоматизовані системи (АС) — системи, що здійснюють автоматизовану обробку даних і до складу яких входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення (ст. 1 Закону від 5 липня 1994 р.).

Під втручанням у роботу АС треба розуміти будь-які дії винного, що впливають на обробку АС інформації, яка в ній зберігається, або яка вводиться чи передається для обробки в АС, тобто дії, що впливають на всю сукупність операцій (зберігання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін по каналах передачі даних. При втручанні в роботу АС здійснюється порушення її роботи, яке спричиняє спотворення процесу обробки інформації, внаслідок чого перекручується або знищується сама інформація чи її носії.

Поняттям "втручання у роботу АС" не охоплюється використання АС для вчинення окремих злочинів. Зокрема, АС можуть використовуватись для виготовлення підроблених грошей, цінних паперів (державних і недержавних), різних документів тощо. У цьому разі АС використовується як знаряддя вчинення іншого злочину. Проте якщо одна АС використовується для втручання у роботу іншої АС, то такі дії є втручанням у роботу АС у розумінні ст. $198^1$ КК.

Знищення інформації — це її втрата, коли інформація в АС перестає існувати для фізичних і юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі. Як знищення, втрату інформації треба розглядати і її блокування, тобто припинення доступу до інформації користувачам АС. Втручання в роботу АС може бути і в формі впливу на канали передачі інформації як між технічними засобами її обробки і зберігання всередині АС, так і між окремими АС, внаслідок чого інформація, що передається для обробки, знищується чи перекручується. Такі дії можуть виражатись, наприклад, в електромагнітному, лазерному і іншому впливі на носії інформації, в яких вона матеріалізується, або по яких вона передається; в формуванні сигналів полів засобів і блоків програм, вплив яких на інформацію, її носії і засоби технічного захисту викликає порушення цілісності інформації, її знищення чи спотворення; у включенні до бібліотек програм спеціальних програмних блоків, зміни програмного забезпечення і інших подібних діях, що призводять до порушення цілісності інформації.

Перекручення інформації — це зміна її змісту, порушення її цілісності, в тому числі і часткове знищення.

Втручання у роботу автоматизованих систем є матеріальним складом злочину, оскільки, крім різноманітних дій у вигляді різного впливу на роботу автоматизованої системи, обов'язковими ознаками його об'єктивної сторони є також наслідки у вигляді перекручення чи знищення інформації, тобто порушення її цілісності (руйнування, спотворення, модифікація і знищення) (абз. 2 п. 2 Положення про технічний захист інформації в Україні); і причинний зв'язок між вчиненими діями і наслідками. Відсутність наслідків у вигляді перекручення або знищення інформації чи носіїв інформації при втручанні у роботу АС, залежно від мети такого втручання, може кваліфікуватися: 1) як замах на вчинення злочину, передбаченого ст. $198^1$, якщо метою втручання було спотворити або знищити інформацію, її носії; 2) за статтями 56, 57, $148^6$ КК (при наявності ознак цих злочинів), якщо метою втручання в роботу АС було незаконне ознайомлення з інформацією, яка в ній обробляється чи зберігається, чи її викрадення, наприклад, шляхом копіювання; 3) за іншими статтями КК, які передбачають відповідальність за злочини, спосіб вчинення яких може виражатись в незаконному втручанні в роботу АС, наприклад, як розкрадання майна, виготовлення з метою збуту чи використання підроблених державних чи недержавних цінних паперів (ст. 79, ч. 3 чи ч. 4 ст. $148^8$). Само по собі умисне незаконне втручання у роботу автоматизованих систем, метою якого не було перекручення чи знищення інформації або носіїв інформації, складу злочину, передбаченого ст. $198^1$ КК, не утворює.

Суб'єктивна сторона злочинів, передбачених ч. 1 ст. 198[1], характеризується прямим умислом щодо вчинюваних винним дій, а психічне відношення винного до наслідків у вигляді перекручення чи знищення інформації або її носіїв може характеризуватись як прямим чи непрямим умислом, так і необережністю в обох видах. При розповсюдженні програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи, умисел лише прямий, оскільки суб'єктивну сторону цього злочину визначає психічне відношення винного до вчинюваних ним дій. Мотиви і мета вчинення злочинів можуть бути різними і свідчити про те, що робота автоматизованої системи порушена, наприклад, з метою вчинення інших злочинів.

Прямий умисел до наслідків у вигляді перекручення чи знищення інформації або її носіїв при втручанні у роботу АС, матиме місце тоді, коли метою такого втручання є, в кінцевому підсумку, перекручення чи знищення інформації, що використовується (обробляється) АС, або знищення носіїв інформації. Непрямий умисел чи необережність у обох її видах щодо наслідків при втручанні в роботу АС матиме місце у випадках, коли втручання мало метою здійснити несанкціонований доступ до інформації для незаконного ознайомлення з нею, наприклад, з метою отримати відомості, що містять державну чи іншу, охоронювану законом, таємницю, наприклад, комерційну таємницю чи відомості конфіденційного характеру, ознайомлення, використання чи розголошення якої може заподіяти шкоду суспільству і державі, юридичним і фізичним особам. Неправомірне отримання інформації з обмеженим доступом, тобто отримання її з порушенням правил розмежування доступу, встановленими власником інформації чи уповноваженою ним особою, може здійснюватись технічними засобами космічної, повітряної, морської і наземної розвідок або шляхом порушення правил розмежування доступу до інформації з обмеженим доступом в АС, засобах обчислювальної техніки, лініях зв'язку — шляхом несанкціонованого доступу до неї (див. п. 25 Положення про технічний захист інформації в Україні). Неправомірне отримання інформації може супроводжуватись перекрученням або знищенням інформації чи носіїв інформації. При цьому особа усвідомлює, що неправомірне отримання інформації може бути поєднане з перекрученням чи знищенням самої інформації чи її носіїв, і, не бажаючи таких наслідків, свідомо допускає їх настання або легковажно розраховує на її ненастання. Втручання в роботу АС, що призвело до перекручення чи знищення інформації або її носіїв, вчинене з метою незаконного отримання інформації, залежно від змісту такої інформації і мети її неправомірного отримання, повинно кваліфікуватися за сукупністю злочинів: ст. 198[1] і, відповідно, за ст. ст. 56, 57 чи 148[6].

Суб’єктом аналізованих злочинів може бути будь-яка фізична осудна особа, що досягла 16-річного віку. Ним можуть бути і особи з персоналу АС — фізичні особи, яких власник АС чи уповноважена ним особа чи розпорядник АС визначили для здійснення функцій управління та обслуговування АС, і сторонні особи. Суб'єктами злочину в формі розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручення або знищення інформації чи її носіїв, можуть бути розробники таких програмних і технічних засобів, їх виготовлювачі, зокрема, виробники (розробники) програм з комп'ютерними вірусами, так звані “технопацюки", "хакери" тощо, в середовищі яких вважається, що чим складніша система захисту в автоматизованій системі, тим престижніше її зламати, і які витрачають на таку діяльність величезну працю і ставлять перед собою єдину мету — спричинити шкоду значній кількості користувачів АС.

Одним із кваліфікованих видів складу злочину, передбаченого ч. 2 ст. 198[1] КК, є спричинення шкоди у великих розмірах внаслідок вчинення передбачених її ч. 1 дій. Визначення розміру заподіяної шкоди при порушенні роботи АС великим залежить від багатьох обставин: 1) вартості інформації чи її носіїв, знищених чи перекручених; 2) збитків, спричинених неможливістю використання знищеної або перекрученої інформації чи її носіїв; 3) затрат на відновлення змісту перекрученої або знищеної інформації чи її носіїв; 4) збитків внаслідок використання неправомірно отриманої інформації тощо. При цьому не повинні враховуватись витрати, які несуть власники, розпорядники і користувачі автоматизованих систем для технічного захисту інформації в них від несанкціонованого доступу до інформації, її приховування, затрати на заходи по технічній дезінформації тощо. При цьому, очевидно, залежно від вартості знищеної чи пошкодженої інформації дії винного можуть додатково кваліфікуватися як умисне знищення чи пошкодження державного, колективного чи індивідуального майна громадян (відповідно статті 89 та 145 КК).

Порушення роботи АС, втручання в її роботу може бути способом вчинення інших, найчастіше більш тяжких, злочинів: диверсії (ст. 60). шпигунства (ст. 57), розкрадання майна (ст. ст. 83. 86[1], 143). виготовлення з метою збуту або використання підроблених державних чи недержавних цінних паперів (ст. 79, ст. 148[8], ч. 3 чи ч. 4) та інші. У таких випадках дії винного повинні кваліфікуватися за сукупністю злочинів: за ст. 198[1] і відповідною статтею КК, яка передбачає відповідальність за злочин, вчинений шляхом втручання в роботу АС.

Як уже зазначалось, умисне втручання у роботу АС може бути вчинене з метою виготовлення, підробки цінних паперів, випущених у бездокументарній формі, їх незаконного використання тощо.

**Цінні папери** — це грошові документи, що засвідчують право володіння або відносини позики, визначають взаємовідносини між особою, яка їх випустила, та їх власником і передбачають, як правило, виплату доходу у вигляді дивідендів або процентів, а також можливість передачі грошових та інших прав, що випливають з цих документів, іншим особам (ч. 1 ст. 1 Закону від 18 червня 1991 р. “Про цінні папери і фондову біржу”

//Відомості Верховної Ради України. – 1991. - № 38. – Ст. 508). До цінних паперів ст. 3 вказаного Закону в редакції від 3 червня 1999 р. віднесені: акції; облігації внутрішніх та зовнішніх державних позик; облігації місцевих позик; облігації підприємств; казначейські зобов'язання республіки; ощадні сертифікати; інвестиційні сертифікати; векселі; приватизаційні папери (Відомості Верховної Ради України. – 1999. - № 31. – Ст. 252). Емітентом цінних паперів може бути держава в особі уповноваженого органу, юридична особа і у випадках, передбачених законодавством, фізична особа. Випуск цінних паперів емітент здійснює від свого імені і зобов'язується виконувати обов'язки, що випливають з умов їх випуску (див. ст. 2 Закону "Про цінні папери і фондову біржу" в редакції від 3 червня 1999 р.). Залежно від того, хто є емітентом цінних паперів, останні можна поділяти на дві групи: 1) державні цінні папери та 2) недержавні цінні папери. Державна комісія з цінних паперів та фондового ринку (далі ДКЦПФР) у роз'ясненні від 20 жовтня 1999 р. № 22 роз'яснила, що до державних цінних паперів відносяться цінні папери, випущені відповідно до законодавства України, та емітентами яких є центральні органи державної влади та управління, що здійснюють фінансово-кредитну діяльність (Українська Інвестиційна Газета. – 1999. – 23 листопада). Державні цінні папери можуть випускатись у формі облігацій внутрішніх та зовнішніх державних позик; казначейських зобов'язань республіки, в тому числі казначейських векселів; приватизаційних паперів. Зазначені цінні папери можуть бути предметом злочину, передбаченого статтею 79 КК.

Цінні папери можуть випускатись як у традиційній паперовій (документарній) формі, так і в бездокументарній формі (див.: Закон України "Про Національну депозитарну систему і особливості електронного обігу цінних паперів в Україні" від 10 грудня 1997 р. // Відомості Верховної Ради України. – 1998. - № 15. – Ст. 67). Форма випуску цінних паперів визначається за рішенням емітента і затверджується ДКЦПФР при реєстрації випуску. Концепцією функціонування та розвитку фондового ринку України, схваленою постановою Верховної Ради України від 22 вересня 1995 р. (Відомості Верховної Ради України. — 1995. — № 33. — Ст. 257) передбачається розширення сфери випуску і обігу як недержавних, так і державних цінних паперів у нематеріалізованій формі, тобто розширення випуску та обігу цінних паперів у бездокументарній формі. Законом України від 30 жовтня 1996 р. "Про державне регулювання ринку цінних паперів в Україні" (Відомості Верховної Ради України. – 1996. - № 15. – Ст. 292) передбачене державне регулювання ринку цінних паперів — здійснення державою комплексних заходів щодо упорядкування, контролю, нагляду за ринком цінних паперів та їх похідних та запобігання зловживанням і порушенням у цій сфері (ст. 1 названого Закону). Підтвердженням права власності на цінні папери, випущені в документарній формі, є сертифікат, а на цінні папери, випущені в бездокументарній формі чи знерухомлені цінні папери (переведені у бездокументарну форму цінні папери, випущені у документарній формі) – виписка з рахунку у цінних паперах, яку зберігач зобов'язаний надавати власнику цінних паперів (див.: абз. 1 ч. 4 ст. 5 Закону "Про Національну депозитарну систему та особливості електронного обігу цінних паперів в Україні"). Виписка про стан рахунку у цінних паперах не є цінним папером, вона є лише підтвердженням права власності на цінні папери на дату стану рахунку, вказану в цій виписці. Така виписка не може бути предметом угод, що тягнуть за собою перехід права власності на цінні папери (див.: абз. 2 ч. 4 ст. 5 Закону "Про Національну депозитарну систему та особливості електронного обігу цінних паперів в Україні"; п. 5.12.1. Положення про депозитарну діяльність, затвердженого рішенням ДКЦПФР від 26 травня 1998 р. № 61 // Українська Інвестиційна Газета. – 1998. – 14 липня). Виписки з рахунку у цінних паперах та виписки із реєстрів власників іменних цінних паперів є офіційним документами, що видаються суб'єктами підприємництва, створеними у формі господарських товариств (депозитарії, зокрема, Національний депозитарій України, та комерційні банки, зберігачі цінних паперів, незалежні реєстратори) або самими емітентами цінних паперів (акціонерними товариствами, які самостійно ведуть власний реєстр власників іменних цінних паперів), а тому їх підробка, в тому числі і незаконне виготовлення з метою збуту, а так само збут чи використання іншим шляхом підроблених виписок, за наявності підстав, може кваліфікуватись за ст. 194 чи ст. 172 КК.

Випуск (емісія) цінних паперів у бездокументарній формі, крім приватизаційних паперів, які засвідчують право власника на безоплатне одержання у процесі приватизації частки майна державних підприємств, державного житлового фонду, земельного фонду здійснюється емітентом шляхом оформлення глобального сертифікату - документу, оформленого на весь випуск цінних паперів, який підтверджує право на здіснення операцій з цінними паперами цього випуску в Національній депозитарній системі. Глобальний сертифікат передається на зберігання в обраний емітентом депозитарій і зберігається у ньому протягом усього періоду існування цінних паперів у бездокументарній формі. На період передплати на певний випуск (емісію) цінних паперів емітент оформляє тимчасовий глобальний сертифікат, який підлягає заміні на постійний після державної реєстрації цього випуску у ДКЦПФР або анулюється в разі визнання випуску таким, що не відбувся (див.: п. п. 3, 4 ст. 4 Закону "Про Національну депозитарну систему та особливості електронного обігу цінних паперів в Україні").

Ч. 3 ст. $148^8$ КК передбачена відповідальність за виготовлення з метою збуту, збут чи використання іншим шляхом підроблених недержавних цінних паперів, а ст. 79 КК – за виготовлення з метою збуту, а також збут підроблених державних цінних паперів. **Під виготовленням** підроблених недержавних цінних паперів треба

розуміти їх створення будь-яким способом. Спосіб виготовлення підроблених недержавних цінних паперів залежить від форми їх існування (документарна чи бездокументарна). Виготовлення підроблених бездокументарних недержавних цінних паперів може бути вчинене шляхом відкриття фіктивного рахунку у цінних паперах у зберігача. Підробкою бездокументарних недержавних цінних паперів слід вважати внесення будь-яких змін до рахунку у цінних паперах у зберігача, які спотворюють зміст зафіксованої у ньому інформації. Такі зміни можуть бути внесені шляхом надання незаконних розпоряджень на здійснення облікових депозитарних операцій (зарахування, списання, переміщення, переказ), наслідком яких може бути зміна кількості цінних паперів на рахунку, обмеження їх в обігу або зняття таких обмежень, чи розпоряджень про внесення змін до реквізитів анкети рахунку у цінних паперах, які не супроводжуються обліковими операціями щодо цінних паперів, наприклад, зміна інформації щодо власника (розпорядника) рахунку тощо.

Виготовлення з метою збуту підроблених бездокументарних цінних паперів, їх підробка чи використання підроблених бездокументарних недержавних цінних паперів, які існують у формі відкритого зберігачем рахунку, здійснюється шляхом внесення неправдивих даних до рахунку в цінних паперах у зберігача на електронних носіях інформації, тобто є одночасно втручанням у роботу автоматизованої системи, якою є така система реєстру. Такі дії одночасно утворюють і склад злочину, передбачений ст. $198^1$, і мають кваліфікуватися залежно від того, хто є емітентом цінних паперів за сукупністю злочинів, передбачених ч. 1 чи ч. 9 ст. 79 або ч. 3 чи ч. 4 ст. $148^8$ та відповідною частиною ст. $198^1$, оскільки при цьому має місце спотворення чи знищення інформації, зокрема, внесення змін в рахунок у цінних паперах, відкритий зберігачем.

З суб'єктивної сторони злочини, передбачені ч. 1 ст. 79 та ч. 3 ст. $148^8$, характеризуються лише умисною виною, а мотиви і мета їх вчинення можуть бути різними. При виготовленні підроблених державних та недержавних цінних паперів обов'язковою ознакою їх суб'єктивної сторони є мета збуту. Залежно від конкретних мотивів і мети виготовлення цінних паперів, а щодо недержавних цінних паперів – також мотивів і мети їх використання, дії винного можуть додатково кваліфікуватися за ст. $198^1$ (якщо предметом є цінні папери у бездокументарній формі), а також як готування до вчинення інших злочинів чи як замах на їх вчинення (наприклад, розкрадання державного, колективного чи індивідуального майна).

**УДК 002.6:342.7:347.777:343.50:35.078**

# ПРОБЛЕМИ ЛАТЕНТНОСТІ КОМП`ЮТЕРНОЇ ЗЛОЧИННОСТІ

***Віталій Цимбалюк***

*Анонація:* **В статті розглядаються питання щодо проблем латентності комп`ютерної злочинності в Україні та за кордоном.**
*Summari*: **In the article the questions concerning problems of a latence of computer crime in Ukraine and abroad are considered.**
*Ключові слова:* **комп`ютерна злочинність, інформаційне право.**

Приблизно з середини XX століття у світі з'явилося нове масове соціально-технічне явище, яке знайшло вираз у категорії "комп`ютеризація" та "інформатизація" і, майже одночасно з ними, виникли нові кримінологічні категорії: "комп`ютерні злочини", "комп'ютерна злочинність", "організована комп`ютерна злочинність". В основі сутності останніх категорій полягає практика використання електронно-обчислювальної (комп`ютерної) техніки та заснованих на ній технологій в різних сферах суспільного життя в антисоціальних цілях.

Комп`ютеризація, на сучасному рівні розвитку, ставить перед суспільством та державою, в тому числі перед правоохоронними органами нові, нетрадиційні проблеми. Серед них особливе місце займають проблеми зростання протиправних проявів у сфері використання комп'ютерних технологій в глобальних комп`ютерних мережах.

Як свідчить історія розвитку світового науково-технічного прогресу, будь-яка технічна новація, зокрема щодо засобів комунікації, завжди, неминуче притягувала до себе людей, які намагалися і намагаються використати її для вчинення злочинів.

Сьогодні у злочинному світі спостерігається нова тенденція: організовані злочинні формування активно освоюють "кіберпростір", відчувши тиск правоохоронних органів на "традиційні" сфери злочинного бізнесу. За оцінками експертів, нині комп'ютерна злочинність набуває такого розвою, що при її ігноруванні в подальшому виникає проблема, щодо загрози окремим інтересам не тільки якоїсь конкретної людини, соціальним приватним