

**Бутузов Віталій Миколайович** — головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, кандидат юридичних наук, старший науковий співробітник

## Співвідношення понять “комп’ютерна злочинність” і “злочинність у сфері високих інформаційних технологій”

*У статті проведено аналіз співвідношення понять “комп’ютерна злочинність” і “злочинність у сфері високих інформаційних технологій”.*

**Ключові слова:** комп’ютерна злочинність, злочинність у сфері високих інформаційних технологій, Інтернет-технології, електронні платежі, телекомунікаційні технології.

Впровадження сучасних інформаційних технологій у сфері економіки, управління, кредитно-банківській діяльності, стрімкий розвиток інформаційно-телекомунікаційних технологій на основі використання глобальної інформаційної мережі Інтернет і спрощення доступу до неї широкого кола користувачів через персональні комп’ютери обумовило поширення високотехнологічних злочинів – злочинів, пов’язаних з використанням високих інформаційних технологій (у тому числі й комп’ютерних).

Сфера високих інформаційних технологій розглядається як сукупність галузей людської діяльності, інформаційні процеси в яких реалізуються методами автоматизованої обробки даних на основі використання інформаційних, телекомунікаційних та інформаційно-телекомунікаційних мереж.

З початку 90-х років минулого століття у діяльності багатьох правоохоронних органів інших країн, зазначає С. Р. Росінська, почали використовуватись терміни “computer crimes” – комп’ютерні злочини або “Hi-tech crime” – злочини у сфері високих технологій, тобто злочини з використанням сучасних інформаційних технологій – комп’ютерних систем, телекомунікацій, систем зв’язку. Аналізуючи спектр

протиправного використання ЕОМ, С. Р. Росінська вказує, що крім злочинних посягань у кредитно-фінансовій сфері, правопорушники все частіше використовують ЕОМ та її периферійні пристрої для фальсифікації різних документів, для зберігання баз даних, що містять кримінальну інформацію про злочин [1].

Тому дослідники розглядають комп'ютерні злочини як підвид злочинів у сфері високих інформаційних технологій [2]. Як правило, це злочини в інформаційній сфері, пов'язані з комп'ютеризованою обробкою інформації.

Відмічається, що ці злочини стали результатом процесу інтенсивного розвитку інформаційної інфраструктури держави, розширення технічних можливостей діючих телекомунікаційних мереж, відсутності у віртуальному просторі територіальних кордонів, а також широкої аудиторії користувачів і можливостей електронної торгівлі. До злочинів у інформаційній сфері відносяться: злочини в сфері комп'ютерної інформації, телекомунікацій і незаконного обороту радіоелектронних і спеціальних технічних засобів [3].

Виходячи із зазначеного, до злочинів у сфері високих технологій можна віднести:

— злочини у сфері комп'ютерної інформації, при вчиненні яких правопорушник використовує одну комп'ютерну інформацію (знаряддя) для здійснення злочинного впливу на іншу комп'ютерну інформацію (предмет);

— злочини, вчинені з використанням у якості знаряддя комп'ютерної техніки та інформаційних технологій;

— злочини, вчинені з використанням у якості знаряддя техніки зв'язку та телекомунікаційних технологій;

— злочини, вчинені з використанням у якості знаряддя техніки та технологій подвійного (інформаційно-телекомунікаційного) призначення.

Злочини у сфері високих інформаційних технологій слід розглядати як злочинні дії, в якості засобів і знарядь учинення яких використовувалися методи автоматизованої обробки інформації, засновані на використанні інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Злочини у сфері високих інформаційних технологій можна визначити як вчинені умисно або з необережності суспільно небезпечні діяння (дії або бездіяльність), що посягають на відносини у сфері обробки інформації в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах, надання та отримання телекомунікаційних послуг, проведення електронних розрахунків.

До найбільш характерних рис злочинності в сфері високих інформаційних технологій можна віднести: високу технічну озброєність

злочинців; високий рівень латентності; використання в якості знарядь злочину інформаційних і телекомунікаційних технологій; електронне середовище, як місце вчинення злочину; транскордонність; організований характер.

На практиці, відповідно до Методичних рекомендацій щодо єдиного порядку обліку злочинів, викритих на визначених пріоритетних напрямках економіки та Єдиного порядку обліку злочинів у сфері економіки [4], комп'ютерні злочини було віднесено до злочинів у сфері високих технологій.

Так, згідно з Методичними рекомендаціями МВС України щодо єдиного порядку обліку злочинів, викритих на визначених пріоритетних напрямках економіки, до злочинів, пов'язаних з сферою високих інформаційних технологій, відносяться (крім злочинів, передбачених розділом XVI КК України), також злочини, передбачені статтями 190, 191, 200, 364, 365, 366, 367, 368, 369 КК України, які вчинені при:

— незаконному втручанні в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж, що призвело до перекручення чи знищення комп'ютерної інформації, а також розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в ці машини, системи чи комп'ютерні мережі й здатних спричинити перекручення або знищення комп'ютерної інформації або носіїв такої інформації;

— підробці документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, а так само придбання, зберігання, перевезення, пересилання з метою збуту піддроблених документів на переказ чи платіжних карток або їх використання чи збут;

— наданні послуг зв'язку та телебачення.

В свою чергу, відповідно до Єдиного порядку обліку злочинів у сфері економіки, до сфери високих технологій, крім злочинів, передбачених розділом XVI КК України, віднесено лише:

— шахрайство, вчинене з використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК України);

— підробку документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, а так само придбання, зберігання, перевезення, пересилання з метою збуту піддроблених документів на переказ чи платіжних карток або їх використання чи збут (ст. 200 КК України).

Узагальнюючи наведене, можна зробити висновок, що в сукупності злочинів у сфері високих інформаційних технологій слід виділити три основні групи злочинів, пов'язаних із застосуванням певних видів високих інформаційних технологій:

- комп'ютерних та Інтернет-технологій;
- технологій електронних платежів;
- телекомунікаційних технологій.

Аналіз злочинів, виявлених підрозділами органів внутрішніх справ у сфері високих інформаційних технологій, дозволяє навести наступну, в залежності від напрямку обслуговування, класифікацію проправних діянь:

1. За напрямком комп'ютерних та Інтернет-технологій – це:
  - безпосереднє або опосередковане (віддалене) несанкціоноване втручання (доступ) у роботу комп'ютерних або телекомунікаційних засобів (мереж);
    - розповсюдження шкідливих програмних засобів у інформаційних і телекомунікаційних мережах та їх подальше використання (наприклад, програми типу “троянський кінь”, замаскованої під іншу програму або документ, які самостійно збирають інформацію про ревізиту потерпілого і пересилають на комп'ютер правопорушника; приховані програми, таємно встановлені у системі потерпілого, які здійснюють заплановані правопорушником шкідливі функції, тощо);
    - використання шкідливих технічних засобів для несанкціонованого втручання у роботу комп'ютерних або телекомунікаційних засобів (мереж) (наприклад, емуляторів таксофонних карток, клонованих SIM-карток тощо);
    - масове розсилання повідомлень електрозв'язку (так званий SPAM в електронних повідомленнях);
    - несанкціоновані дії з інформацією, яка обробляється комп'ютерними засобами або пересилається каналами зв'язку;
    - перехоплення або копіювання інформації, яка обробляється комп'ютерними засобами, передається каналами зв'язку (перехоплення здійснюється через зовнішні комунікаційні канали системи або шляхом безпосереднього підключення до ліній периферійних пристроїв; правопорушнику безпечніше здійснити підключення технічних засобів до інформаційних і телекомунікаційних систем через мережі законних користувачів по каналах електрозв'язку; сучасні технічні засоби дозволяють одержувати інформацію без безпосереднього підключення до комп'ютерної системи: за рахунок перехоплення випромінювань центрального процесора, дисплея, комунікаційних каналів, принтера тощо);
    - порушення встановлених правил експлуатації комп'ютерних і телекомунікаційних засобів (іноді має місце змова правопорушника з працівниками, які відповідають за їх експлуатацію);
    - порушення порядку або правил захисту інформації, яка обробляється комп'ютерними засобами, передається каналами зв'язку (наприклад,

### ***Боротьба з організованою злочинністю і корупцією (теорія і практика)***

---

помста колишніх працівників, які мали доступ до комп'ютерної мережі та скористалися паролями, якщо вони не були своєчасно змінені);

— ініціювання переказів коштів за товар (послугу), проданий у мережі Інтернет, за відсутності товару (послуги).

2. За напрямком електронних платежів це:

— збирання, у тому числі з використанням технічних засобів, інформації, що становить комерційну (банківську) таємницю (про реквізити справжніх платіжних карток, засоби (паролі, логіни) доступу до електронних рахунків тощо);

— шахрайське використання справжніх платіжних карток (платіжних документів);

— підроблення платіжних карток (платіжних документів);

— ініціювання неналежних міжнародних поштових відправлень шляхом використання реквізитів справжніх платіжних карток для оплати товарів у мережі Інтернет;

— ініціювання неналежних переказів коштів шляхом використання: підроблених платіжних карток (платіжних документів); реквізитів справжніх платіжних карток;

— надання незаконних банківських і фінансових послуг у мережі Інтернет.

3. За напрямком телекомунікаційних технологій:

— ухилення від належної оплати за отримані послуги зв'язку (шахрайство абонентів) (наприклад несанкціоноване використання каналів телекомунікаційного зв'язку через перепрограмування стільникового (мобільного) телефону (або клонування SIM-картки), після чого злочинець буде використовувати телефон, а рахунки будуть отримувати інші особи чи організації);

— стягнення оплати за ненадані послуги зв'язку (шахрайство операторів);

— порушення маршрутизації міжнародного (міжміського) телефонного трафіку (направлення міжнародного телефонного трафіку на телефонну мережу загального користування України під виглядом місцевих з'єднань);

— надання без ліцензії послуг зв'язку (особливо міжнародного) (наприклад, із використанням технології IP-телефонії, суть якої полягає в цифровій обробці електричних сигналів телефонних розмов (розділення цифрового сигналу голосової телефонії на окремі пакети даних у пункті передачі та об'єднанні пакетів у певному порядку в пункті прийому);

— використання без ліцензії радіочастотного ресурсу України.

Таким чином, можна дійти висновку, що комп'ютерну злочинність слід розглядати в якості підсистеми злочинності у сфері високих інформа-

ційних технологій, яка пов'язана із протиправним використанням саме комп'ютерних технологій автоматизованої обробки інформації.

### *Список використаних джерел*

1. Россинская Е. Р. Компьютерные преступления : уголовно-правовые и криминалистические аспекты / Е. Р. Россинская // Воронежские криминалистические чтения / [под ред. О. Я. Баева]. — Воронеж : Изд. Воронеж. гос. ун-та, 2002. — Вып. 3. — С. 169–170.
2. Шеломенцев В. П. Високі інформаційні технології та загрози їх кримінального використання / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). — 2009. — № 20. — С. 274–283. ; Шеломенцев В. П. Поняття злочинів у сфері високих технологій / В. П. Шеломенцев // Правова держава : історія, сучасність та перспектива формування в Україні : всеукр. наук.-практ. конф. (м. Запоріжжя, 24 квіт. 2009 р.) : матеріали [у 2-х ч.]. — Запоріжжя : Юрид. ін-т ДДУВС, 2009. — Ч. 2. — С. 168–171.
3. Ишин А. М. О некоторых тенденциях развития криминалистики в современных условиях / А. М. Ишин // Вестник криминалистики / [отв. ред. А. Г. Филиппов]. — М. : Спарк, 2006. — Вып. 4 (20). — С. 34.
4. Методичні рекомендації щодо єдиного порядку обліку злочинів, критичних на визначених пріоритетних напрямках економіки від 2 січ. 2003 р. ; Єдиний порядок обліку злочинів у сфері економіки від 20 черв. 2004 р.

*В стат'ї проведено аналіз соотношения понять “компьютерная преступность” и “преступность в сфере высоких информационных технологий”.*

*The article is devoted to the analysis of the correlation of the concepts “computer crime” and “crime in high information technology sphere”.*

*Стаття надійшла до редакції журналу 25 листопада 2010 року.*