**Андрій Мальгівський, Ельдар Даврушев**

**(Харків, Україна)**

**КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ**

«Кіберзлочинність», «хакери», «комп’ютерний злом», «крадіжка машинного часу» - ці терміни вже перестали бути екзотикою для юристів. Проблеми протидії злочинам  у сфері використання комп’ютерної техніки активно обговорюється науковцями, досить швидко розвивається практика застосування відповідних норм законодавства про кримінальну відповідальність.

На сьогодні комп’ютерні злочини - це одна з найдинамічніших груп суспільно небезпечних посягань . Швидко  збільшуються показники поширення цих злочинів, а також постійно зростає їх суспільна небезпечність. Це зумовлене прискореним розвитком науки й технологій у сфері комп’ютеризації, а також постійним і стрімким розширенням сфери застосування комп’ютерної техніки. Слід зауважити , що український законодавець приділяє значну увагу цій проблемі: новий Кримінальний кодекс України вперше передбачив самостійний розділ про ці злочини - розділ ХVI «Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж»; двічі положення цього розділу змінювалися і доповнювалися – це свідчить про актуальність цієї проблеми в суспільстві.

Сучасний світ практично неможливо уявити без нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та новітніх засобів комунікацій. Сьогодні комп'ютери впроваджуються в різноманітні галузі людської діяльності. Усі найважливіші функції сучасного суспільства, так чи інакше, пов’язані з комп'ютерами, комп'ютерними мережами і комп'ютерною інформацією. Останнім часом в Україні значно зросла кількість Інтернет користувачів, адже підключення до глобальної мережі стало доступним та зручним. Сьогодні персональний комп’ютер, КПК, мобільний телефон з підключенням до Інтернету сприймається як належне та необхідне. Популярність Інтернету невипадкова, адже він забезпечує цілодобовий доступ до величезної кількості інформації, швидку передачу даних, можливість проведення банківських, торгових, біржових операцій, переказ коштів і багато іншого. Інтернет – це чудовий засіб для зв’язку та спілкування. Для багатьох людей він став цілим світом, віртуальним світом. Як і в реальному світі, так і в віртуальному, де панує комп’ютерна інформація, трапляються, злочини, кіберзлочини.

Розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем - це далеко не повний перелік подібних злочинів. Дану категорію злочинів називають по-різному: кіберзлочини, комп’ютерні злочини, злочини в сфері комп’ютерних технологій, злочини в сфері комп’ютерної інформації. В літературі найчастіше зустрічаються два терміни: кіберзлочини та комп’ютерні злочини. Оскільки вони використовуються для назви одних і тих самих суспільно-небезпечних діянь, то їх можна вважати синонімами та рівнозначними. У зв’язку з ратифікацією Україною Конвенції «Про кіберзлочинність» від 7 вересня 2005 року вважається за доцільне вживати термін кіберзлочини. Поняття “кіберзлочин” молоде і утворено сполученням двох слів: кібер і злочин. Термін “кібер” має на увазі поняття кіберпростору та інформаційний простір, що моделюється за допомогою комп’ютера. Тобто кіберзлочини – це суспільно-небезпечні діяння, які так чи інакше пов’язані з кіберпростором та комп’ютерною інформацією, що моделюється комп’ютерами. Такі злочини характеризуються наступними особливостями: високою латентністю, складністю їх виявлення та розслідування, складністю доказу в суді подібних справ, транснаціональною складовою в основному з використанням інформаційної мережі Інтернет, високим збитком навіть від одиничного злочину.

Криміналістична особливість кіберзлочинів заключається в тому, що розслідування та розкриття цих злочинів неможливе без застосування та використання комп’ютерних технологій. Це пов’язано з необхідністю відшукування, фіксування, вилучення та збирання доказів в електронній формі. Також комп’ютерні технології широко використовуються для проведення оперативно-розшукових заходів.

Кіберзлочини можна класифікувати на два види: традиційні злочини, що вчиняються за допомогою комп’ютерних технологій та Інтернету(шахрайство з використанням ЕОМ, незаконне збирання відомостей, що становлять комерційну таємницю, шляхом несанкціонованого доступу до комп'ютерної інформації і т.д.), та нові злочини, що стали можливі завдяки новітнім комп’ютерним технологіям (злочини передбачені Розділом ХVI Кримінального кодексу України). Найчастіше з використанням комп’ютера та Інтернету вчиняються такі традиційні злочини: порушення авторського права і суміжних прав(ст. 176); шахрайство (ст. 190); незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення (ст. 200); ухилення від сплати податків, зборів (обов'язкових платежів)(ст. 212); ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301); незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231). Отже в криміналістичному аспекті кіберзлочини – це передбачені кримінальним законом суспільно небезпечні діяння, для скоєння та розслідування яких застосовуються комп’ютерні технології та/або використовується глобальна мережа Інтернет.

Кіберзлочинність - це злочинність у так званому «віртуальному просторі». Віртуальний простір можна визначити як простір, що моделюється за допомогою комп'ютера інформаційний, у якому перебувають відомості про особи, предмети, факти, подіях, явищах і процесах, представлені в математичному, символьному або будь-якому іншому виді й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі.

Першою причиною розвитку кіберзлочинності, як і будь-якого бізнесу, є прибутковість, – вона неймовірно прибуткова. Величезні суми грошей з'являються в кишенях злочинців у результаті окремих великих афер, не говорячи вже про невеликі суми, які йдуть просто потоком. Друга причина росту кіберзлочинності як бізнесу - те, що успіх справи не пов'язаний з більшим ризиком. У реальному світі психологічний аспект злочину припускає наявність деяких коштів стримування. У віртуальному світі злочинці не можуть бачити своїх жертв, будь те окремі люди або цілі організації, які вони вибрали для атаки. Грабувати тих, кого ти не бачиш, до кого не можеш дотягтися рукою, набагато легше.

У кожного покоління злочинців свої інструменти. Сучасні кіберзлочинці вибрали своєю зброєю троянські програми, за допомогою яких вони будують ботмережі для крадіжки паролів і конфіденційної інформації, проводять до атаки й шифрують дані, щоб потім шантажувати своїх жертв. Характерною й небезпечною рисою сьогоднішніх шкідливих програм є те, що вони прагнуть зберегти свою присутність на інфікованій машині. Для досягнення цієї мети злочинці використовують різні технології. Інша розповсюджена технологія, використовувана в шкідливих програмах, - порушення роботи антивірусних програм для запобігання виявлення шкідливого ПО й продовження його існування на комп'ютері. Такі дії часто спрямовані на припинення забезпечення безпеки, видалення коду або модифікацію хостових файлів Windows для припинення відновлення антивірусних. Серед установ, які намагаються максимально швидко брати на озброєння технологічні новинки, чільне місце посідають банки. Вони мало не щомісяця пропонують нам сервіси, що дозволяють максимально легко і просто розпоряджатися своїми грошима. Платіжні карти і банкомати вже давно стали частиною нашого життя, а інтернет-банкінг, купівля товарів через всесвітню мережу – не «заморська» екзотика. На жаль, цим користуються не лише клієнти, а й злочинці.

Кіберзлочинність – явище новітньої, цифрової доби. Саме це й робить «кіберів» набагато небезпечнішими й ефективнішими за своїх «класичних» колег-шахраїв.

Це люди, які працюють головою і роблять свої «справи», не відходячи від свого комп’ютера або сидячи на лавочці з ноутбуком і мобільним телефоном. Для сучасних «технарів» це часто ідеальний спосіб заробити і реалізувати себе.  Злочинці не стоять на місці. Їхні методи вдосконалюються і стають дедалі складнішими. Відповідно, реагують і правоохоронці.

Останнім часом рівень кіберзлочинності швидко зростає в Україні.

Однак, на думку експертів, кіберзлочинність не є негайною загрозою для українців. Наша країна в особливому становищі, адже має один із найнижчих у Європі рівнів підключення до Інтернету.

Україна – не виняток. Зі зростанням обсягів безготівкових розрахунків зростає і кількість потерпілих від кібершахраїв.

Наша країна з її низьким рівнем обізнаності про загрози використання комп'ютерів і низьким рівнем інформаційної безпеки стає для них справжнім клондайком. Так, за оцінками експертів, в останні місяці в управлінні з боротьби з кіберзлочинністю тільки в Києві фіксується до двадцяти випадків крадіжки грошей через клієнт-банк. Суми становлять від 20 тис. до 40 млн. грн. Однак подібні факти замовчуються, повідомлень в ЗМІ про них практично немає. Ні потерпілим, ні банкам, ні міліції не вигідний галас навколо того, що відбувається. У ряді випадків бувають ситуації, коли такі шахрайські схеми реалізуються організованими групами, у які входять представники банків та силових структур.

Українською проблемою є як недостатня кількість державних експертів в області комп'ютерно-технічної експертизи, так і складнощі з введенням в правове поле досліджень фахівців комерційних організацій. Типовий термін проведення комп'ютерно-технічних експертиз становить від півроку і вище через високу завантаженість профільних державних установ. Весь цей час підозрюваний може перебувати в СІЗО.

На все це накладається набуття чинності 19 листопада 2012 року нового КПК, який встановлює нові і поки «незрозумілі» правила взаємодії всіх учасників процесу. У зв'язку з посиленням європейського законодавства кіберзлочинці можуть перекочувати в менш захищену Україну.

Таку думку висловив директор департаменту захисту інтелектуальної власності Microsoft Юрій Омельченко під час Міжнародної конференції Computer Forensics Ukraine 2012 в Києві, передав кореспондент ГолосUA.

За його словами, у світі боротьба з кіберзлочинністю, однозначно, посилюється. Так, зокрема, Європа і США ідентифікували цю проблему як одну з найбільш небезпечних і ухвалюють велику кількість нормативних документів для захисту інформації від кіберзлочинності.

Українське ж законодавство у сфері захисту інформації, на думку Ю. Омельченка, вимагає дуже серйозного доопрацювання. «Потенційно існує ймовірність того, що кіберзлочинність буде виштовхуватися з Європи, то вона буде перебиратися в Україну. Та й уже цей процес відбувається», - зазначив експерт.

При цьому директор департаменту Microsoft відзначив, що іноземці дуже високо цінують українські «світлі голови» і щосили вже використовують їх знання для вчинення протиправних дій. У зв'язку з цим представник СБУ Тарас Бєлов нагадав, що минулого року правоохоронні органи «розібралися» з цілою групою таких осіб, які продавали свої - дуже висококласні - хакерські розробки за кордон.

Таким чином, кіберзлочинність - це проблема, з якою зіштовхнулась планета у 21 столітті, і яка обіцяє рости та поглинати все більше коштів. Незважаючи на усі заходи, що їх приймають окремі особи, фірми, а також держава, кіберзлочинність продовжує свою діяльність, збільшуючи прибутки порушників та зменшуючи вміст кишень пересічних громадян. Тому сьогодні особливо важливо переглянути усі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців.

Термін «кіберзлочинність» в офіційних нормативно-правових документах не визначений. Разом з тим, саме поняття закріпилося в лексиконі правоохоронних органів розвинених держав Європи і світу і має на увазі злочинність у сфері комп'ютерної інформації і телекомунікацій, незаконний обіг радіоелектронних і спеціальних технічних засобів, поширення неліцензійного програмного забезпечення для ЕОМ, а також деякі інші види злочинності.

Нині кіберзлочинність становить для нашої держави більш серйозну небезпеку, ніж ще 5 років тому. Незважаючи на зусилля правоохоронних органів, спрямованих на боротьбу з кіберзлочинами, їх кількість, на жаль, не зменшується, а, навпаки, постійно збільшується.

Хоча аналіз національного законодавства України, що регулює суспільні інформаційні відносини, дозволяє стверджувати, що наша держава вживає необхідних заходів, спрямованих на профілактику та протидію комп'ютерної злочинності. Прикладом цьому може служити Указ Президента від 31 липня 2000 року «Про заходи розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в Україні», а також Розділ 16 «Злочини у сфері використання електро-обчислюваних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку систем та комп'ютерних мереж» чинного Кримінального кодексу України. Верховною Радою України був прийнятий за основу проект Закону «Про внесення змін до Кримінально-процесуального кодексу України», відповідно до якого будуть розширені можливості Служби безпеки України при розслідуванні порушень в роботі автоматизованих систем. Але цього вияляється не достатньо для повного подолання кіберзлочинності в нашій країні.

Проблема профілактики і стимулювання кіберзлочинності в Україні – це комплексна проблема. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері. Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній.

**Науковий керівник:**

кандидат юридичних наук, доцент Леонтьєва Л.В.