Бориспільський міськрайонний суд Київської області
08300, м. Бориспіль, вул. Київський шлях, 72, тел./факс (04595) 6-76-19,
inbox@bpm.ko.court.gov.ua

7 липня 2015 року № _____

Секретарю судової палати
розгляду кримінальних справ
апеляційного суду
Київської області

Ю.М.Сливі

Узагальнення судової практики
розгляду Бориспільським міськрайонним судом кримінальних проваджень про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (розділ XVI Особливої частини Кримінального кодексу України) за 2012-2014 роки.

На виконання листа Апеляційного суду Київської області №14157/07-16/15 від 23.06.2015 року Бориспільським міськрайонним судом було проведено узагальнення судової практики розгляду судом кримінальних проваджень про злочини у сфері використання електронно-обчислювальних машиин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозвязку за 2012-2014 роки.

Метою проведення узагальнення є висвітлити проблемні питання, що виникають при розгляді вказаних кримінальних проваджень, а також проаналізувати практику розгляду кримінальних проваджень про шахрайство з використанням електронно-обчислювальної техніки, шахрайство з банківськими картками.

Комп'ютерна злочинність — це особливий вид злочинів, пов'язаних із незаконним використанням сучасних інформаційних технологій і засобів комп'ютерної техніки. В їх основі можуть бути політичні, хуліганські, корисливі й інші мотиви. Це зумовлює необхідність розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності. Інформаційні відносини, тобто відносини, що виникають при одержанні, використанні, поширенні та зберіганні інформації, регулюються положеннями Конституції України, законами від 2 жовтня 1992 р. № 2657-XII «Про інформацію», від 25 червня 1993 р. № 3322-XII «Про науково-технічну інформацію», від 18 листопада 2003 р. № 1280-IV «Про телекомунікації», від 5 липня 1994 р. № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах» (в редакції Закону від 31 травня 2005 р. № 2594-IV), а також низкою підзаконних актів, зокрема Положенням про технічний захист інформації в Україні (затверджене Указом Президента України від 27 вересня 1999 р. № 1229/99) та ін.

Згідно з чинним законодавством України кримінальну відповідальність за злочини у сфері використання електронно-обчисолювальних машин, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку передбачено у розділі XVI Кримінального кодексу України.

В Україні найбільш поширеним злочином у сфері використання електронно-обчислювальних машин, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку є злочин, відповідальність за який передбачено ст. 361 КК («Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»). У цій статті передбачено відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підроблення, блокування інформації, спотворення процесу автоматичної обробки інформації або до порушення встановленого порядку її маршрутизації.

Об'єктом такого злочину є електронно-обчислювальні машини, автоматизовані системи, комп'ютерні мережі та мережі електрозв'язку. Об'єктом такого злочину також може бути право власності на комп'ютерну інформацію. Для визнання факту вчинення злочину, склад якого передбачено у ст. 361 КК, суд має встановити не лише вчинення діяння, а й настання хоча б одного із зазначених в законі наслідків: витоку, втрати, підроблення, блокування інформації, спотворення процесу її обробки або порушення встановленого порядку її маршрутизації. Тобто між несанкціонованим втручанням в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку має бути причинний зв'язок хоча б з одним із суспільно небезпечних наслідків. Специфіка розгляду справ цієї категорії полягає у правильному розумінні термінів, визначення яких містяться у наведених вище нормативних документах.

Електронно-обчислювальна машина розуміється як комплекс електронних технічних засобів, побудованих на основі мікропроцесорів і призначених для автоматичної обробки інформації при вирішенні обчислювальних та інформаційних завдань.

Автоматизована система – організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей і персоналу, що здійснює цю діяльність. Зокрема, такими системами слід вважати сукупність ЕОМ, засобів зв'язку та програм, за допомогою яких ведеться документообіг, формуються, оновлюються та використовуються бази даних, накопичується та обробляється інформація. Оскільки обробка певних даних можлива і в результаті роботи одного комп'ютера, то автоматизована система - це й окремо взятий комп'ютер разом з його програмним забезпеченням.

Комп'ютерна мережа — це сукупність програмних і технічних засобів, за допомогою яких забезпечується можливість доступу з однієї ЕОМ до програмних чи технічних засобів інших ЕОМ та до інформації, що зберігається у системі іншої ЕОМ.

Мережа електрозв'язку — комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

Об'єктивна сторона злочину проявляється у формі несанкціонованого втручання в роботу електронно-обчислю.вальних машин, їх систем, комп'ютерних мереж чи мереж електрозв'язку, наслідком якого є: 1) витік; 2) втрата; 3) підроблення; 4) блокування інформації; 5) спотворення процесу автоматичної обробки інформації; 6) порушення встановленого порядку її маршрутизації.

Несанкціоноване втручання в роботу ЕОМ, їх систем чи комп'ютерних мереж — це проникнення до цих машин, їх систем чи мереж і вчинення дій, які змінюють режим роботи машин, їх систем чи комп'ютерних мереж або повністю чи частково припиняють їх роботу без дозволу відповідного власника або уповноваженої особи.

Несанкціонованим втручанням в роботу мереж електрозв'язку слід вважати будь-які (окрім втручання в роботу ЕОМ, їх систем чи комп'ютерних мереж, що забезпечують роботу мереж електрозв'язку) вчинені без згоди власника відповідної мережі чи службових осіб, на яких покладено забезпечення її нормальної роботи, дії, внаслідок яких

припиняється (зупиняється) робота мережі електрозв'язку або відбуваються зміни режиму цієї роботи.

Комп'ютерна інформація — це текстова, графічна чи будь-яка інша інформація (дані), яка існує в електронному вигляді, зберігається на відповідних носіях і може бути створена, змінена чи використана за допомогою ЕОМ.

Залежно від засобів інформаційні відносини, які є родовим об'єктом досліджуваних злочинів, можуть бути поділені на чотири види:

1) інформаційні відносини, засобом забезпечення яких є комп'ютери;

2) інформаційні відносини, засобом забезпечення яких є комп'ютерні системи;

3) інформаційні відносини, засобом забезпечення яких є комп'ютерні мережі;

4) інформаційні відносини, засобом забезпечення яких є мережі електрозв'язку.

Статті 361 – 362 та 363-1 КК України містять такі спільні кваліфікуючі ознаки:

- вчинення комп'ютерного злочину повторно;

- вчинення комп'ютерного злочину за попередньою змовою групою осіб;

- вчинення комп'ютерного злочину, який заподіяв значну шкоду.

Оскільки в розділі XVI Особливої частини КК України не передбачено повторності однорідних злочинів, комп'ютерний злочин слід вважати вчиненим повторно у випадках, коли особа два або більше рази вчинила злочин, який було кваліфіковано за однією статтею даного розділу. При цьому вчинення декількох таких злочинів не охоплювалося єдиним умислом (злочин не був продовжуваним), особа не звільнялася від кримінальної відповідальності за тотожний злочин, не закінчилися строки давності притягнення до кримінальної відповідальності за раніше вчинений злочин або судимість за нього не було погашено чи знято.

Комп'ютерний злочин буде вважатися вчиненим групою осіб за попередньою змовою за наявності відповідних об'єктивних і суб'єктивних ознак. Об'єктивна сторона його може бути такою:

- діяння вчиняється двома або більше виконавцями, кожен із яких виконує всі дії, що утворюють об'єктивну сторону складу (наприклад, декілька осіб здійснюють несанкціоноване втручання з окремих терміналів і знищують певну інформацію);

- злочин вчиняється двома або більше співвиконавцями, кожен із яких виконує частину дій, що характеризують об'єктивну сторону (наприклад, одна особа вчиняє несанкціоноване втручання й перекручує комп'ютерну інформацію про користувачів комп'ютерної мережі та паролі їх доступу, а інша знищує комп'ютерну інформацію);

- злочин вчиняється двома або більше особами, при цьому лише одна з них відіграє роль виконавця, а інші є підбурювачами, пособниками або організаторами (наприклад, одна особа забезпечує іншу необхідним устаткуванням, а остання вчиняє розповсюдження шкідливої комп'ютерної програми).

При цьому кожен із співвиконавців повинен мати всі ознаки суб'єкта, тобто бути фізичною, осудною особою та досягти віку кримінальної відповідальності[x]. У випадку, коли особа не була поінформована про те, що вчиняє комп'ютерний злочин разом із малолітнім або неосудним, її дії слід кваліфікувати за правилами фактичної помилки як замах на вчинення комп'ютерного злочину групою осіб за попередньою змовою.

До об'єктивних ознак вчинення злочину за попередньою змовою групою осіб відноситься також спільність, що характеризується взаємозумовленістю дій, загальним для всіх співучасників наслідком і наявністю причинового зв'язку між діями співучасників і злочином, який вчинив виконавець.

Певну специфіку має суб'єктивна сторона комп'ютерного злочину в разі його вчинення за попередньою змовою групою осіб. Домовленість про спільне вчинення цього

злочину може бути досягнута без особистого знайомства співвиконавців. У практиці російських правоохоронних органів мав місце випадок, коли за допомогою комп'ютерної мережі Інтернет рядом осіб було вчинено розкрадання, причому ці суб'єкти один одного особисто навіть не бачили, оскільки спілкувалися за допомогою електронної мережі, у якій кожен мав свій псевдонім[xi].

Значною шкодою в статтях 361 – 363-1 КК, якщо вона полягає в заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів (примітка до статті 361 КК). Зазвичай ця шкода полягає в заподіянні позитивних матеріальних збитків. У такому випадку її необхідно оцінювати, виходячи з витрат власника на придбання комп'ютерної інформації. Але стосовно значної шкоди як кваліфікуючої ознаки комп'ютерного злочину слід зауважити, що іноді вона може виражатися і в упущеній вигоді. Це пояснюється тим, що на сучасному етапі будь-яка діяльність як необхідний елемент включає інформаційне забезпечення. Ефективність діяльності багато в чому залежить від кількості та якості вхідної інформації[xii], тому перекручення або знищення інформації, що має порівняно невелику ціну, здатне заподіяти значних матеріальних збитків у вигляді упущеної вигоди. Саме тому видається правильним, крім втрати або зменшення обсягу інформації, якою володіє потерпілий, у розмір матеріальних збитків від комп'ютерного злочину включати також і упущену вигоду, яка може полягати в укладанні невигідних договорів, падінні авторитету, невиконанні умов договорів тощо.

Крім матеріальної шкоди, суспільно небезпечні наслідки при вчиненні комп'ютерного злочину можуть виражатись і в нематеріальних видах шкоди, що зумовлено використанням ЕОМ, систем і комп'ютерних мереж для контролю над складними технологічними процесами, об'єктами та керування ними. Це така шкода, як порушення нормальної роботи підприємств, зупинення або порушення складних технологічних процесів, погіршення обороноздатності держави, підрив авторитету державних органів, підприємств, установ або організацій, створення загрози або заподіяння шкоди життю та здоров'ю громадян, порушення безпеки руху транспорту тощо. Суб'єктивна сторона комп'ютерного злочину, який заподіяв істотну шкоду характеризується змішаною формою вини. У таких злочинах психічне ставлення особи до діяння та першого, обов'язкового, наслідку (втрати, підробки, блокування інформації тощо) виражається в умислі (прямому або непрямому), а до другого (кваліфікованого) наслідку – істотної шкоди – може бути як умисним так і необережним. При цьому зауважимо, що в деяких випадках, умисне заподіяння істотної шкоди в результаті комп'ютерного злочину може фактично представляти собою інший склад злочину.

За період 2012-2014 року Бориспільським міськрайонним судом Київської області було розглянуто одне кримінальне провадження щодо злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку".

Відповідно, вироком (угода про визнання винуватості) від 1 жовтня 2014 року було затверджено угоду, укладену між прокурором, який підтримує обвинувачення та обвинуваченим на наступних умовах: Та.-ра В.В. визнати винним у скоєнні злочину, передбаченого ч. 1 ст. 361-1 КК України та призначити покарання у виді 11 950 грн. штрафу в дохід держави, без позбавлення права обіймати певні посади чи займатися певною діяльністю, з конфіскацією ноутбука «Соні» в дохід держави. Стягнути із засудженого на користь Державного бюджету України 3694 грн. 33 коп. судових витрат.

При цьому суд виходив з того, що обвинувачений Та.-р В.В., в період з січня по липень 2013р. перебуваючи по місцю свого проживання в будинку № 5 по вул.Сонячній в с.В.Олександрівка Бориспільського району Київської області, використовуючи свій власний ноутбук «Соні», моделі SVZ1311CHXXI, серійний номер 543054790000573 з можливістю доступу до мережі Інтернет, а також власний досвід у створенні програмного забезпечення на мові програмування «Visual C++», умисно, шляхом написання вихідних кодів створив функціональні модулі(складові частини) шкідливого програмного засобу під

назвою «ZeuS 2.0.8.9.» у вигляді електронного файлу «zsb.exe», за допомогою якого, вказана шкідлива програма могла несанкціоновано потрапляти на комп»ютер фізичної чи юридичної особи, де без відома вказаних осіб серед інформації, яка обробляється і зберігається на вказаному комп'ютері, автоматично відшуковувати будь-яку інформацію, у тому числі і паролі та ключі доступу до програмного забезпечення «клієнт-банк», а також щодо банківських рахунків, а після відшукання необхідної інформації, самостійно та несанкціоновано, тобто без дозволу власника комп'ютера, пересилатиме її через мережу Інтернет на сервер, заздалегідь визначений користувачем даної шкідливої програми, а також через мережу Інтернет буде надавати своєму користувачеві віддалений доступ до цього комп'ютера, за допомогою якого ним можливо було повністю управляти із будь-якого місця та без відома власника.

Таким чином, обвинувачений Та.-р В.В. вчинив створення з метою розповсюдження шкідливого програмного засобу, призначеного для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), тобто злочин, передбачений ч. 1 ст. 361-1 КК України.

Прокурор та обвинувачений звернулись до суду з угодою про визнання винуватості, в якій просять затвердити дану угоду та призначити покарання обвинуваченому, у виді 750 неоподаткованих мінімумів доходів громадян з конфіскацією ноутбука.

Суд, розглянувши дану угоду, заслухавши думку учасників судового розгляду, дослідивши інші матеріал справи, прийшов до висновку, що слід затвердити дану угоду на умовах викладених письмово, оскільки обвинувачений обвинувачується у вчинені злочину середньої тяжкості, сторони згодні з обвинуваченням, узгодили покарання та умови його відбуття, ознайомлені та усвідомлюють наслідки укладення та затвердження даної угоди на вказаних умовах відповідно до ст.ст.394, 424, 473 КПК України, а також наслідки її невиконання на підставі тс.476 КПК України, а тому суд затвердив угоду, укладену між прокурором та обвинуваченим.

Аналізуючи практику призначення покарань за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку необхідним є зазначити, що судді Бориспільського міськрайонного суду в цілому правильно застосовуються норми кримінально-процесуального та кримінального права з метою охорони прав та законних інтересів осіб, покарання призначались в межах санкцій статей КК України.

Отже, надати спірні питання застосування норм процесуального права не маємо можливості, так як у провадженні Бориспільського міськрайонного суду Київської області у період з 2012 -2014 року перебувало лише одне кримінальне правопорушення даної категорії по обвинуваченню однієї особи з постановленим вироком (угодою про визнання винуватості) від 01.10.2014 року.

Також повідомляємо, що лист від 23.06.2015 року щодо проведення даного узагальнення надійшов до суду електронною поштою лише 06.07.2015 року, тому провести узагальнення до 03.07.2015 року не надалось можливим.

З повагою

Голова
Бориспільського міськрайонного суду
Київської області **Вознюк С.М.**