Хоменко О.М., студентка Національного університету ДПС України Топчій В.В., доктор юридичних наук, доцент, заслужений юрист України, завідувач кафедри кримінального права та кримінології Національного університету ДПС України

Деякі проблеми розслідування та попередження кіберзлочинності

У XXI столітті нова історична фаза розвитку цивілізації - інформаційне суспільство поступово набирає обертів, несучи з собою не тільки позитивні, а й негативні тенденції та явища. Не можливо не звертати увагу на важливість інформаційних технологій, які стали супутником сучасної людини не лише на робочому місці, а й заполонили майже всі сфери життєдіяльності. Разом із зручністю і швидкістю сучасних засобів зв'язку,на сучасному етапі розвитку суспільних, культурних та економічних відносин в Україні збільшилася кількість так званих кіберзлочинів.

Кіберзлочинність - це злочинність у так званому «віртуальному просторі». Віртуальний простір або кіберпростір можна визначити як змодельований за допомогою комп'ютера інформаційний простір, в якому знаходяться відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому вигляді і що знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки і передачі.

Метою роботи є дослідження деяких проблем, що перешкоджають розслідуванню та попередженню кіберзлочинності, а також вироблення пропозицій щодо їх вирішення.

На відміну від традиційних видів злочинів, кіберзлочинність явище відносне молоде і нове,яке виникло з появою мережі Інтернет. Слід зазначити,що сама природа цієї мережі є достатньо сприятливою для вчинення злочинів. Сьогодні найбільше увага злочинців зосереджена на спробах порушення роботи або несанкціонованого використання можливостей інформаційно-телекомунікаційних систем державного, кредитно-банківського, комунального, оборонного, виробничого секторів.

Якщо звернутись до витоків історії то стає зрозумілим,що найбільшого розвитку ці злочини набули з вісімдесятих років,коли Фред Коен вперше опублікував відомості про розробку комп'ютерних вірусів та їх дію на інші комп'ютери. У 1986 році в Сполучених Штатах Америки вперше прийнято закон «The Computer Fraudand Abuse AC»,який забороняв неавторизований доступ до будь-якої комп'ютерної системи і отримання секретної військової інформації. [6]

Прецедентом вчинення даного злочину в Україні є «справа Володимира Льовіна». Цей злочин учинено групою осіб,які скориставшись мережею Інтернету, здійснила 40 грошових переказів на загальну суму 10 млн. 700 тис 952 доларів США з рахунків осіб, що знаходились в різних країнах (США,Фінляндія,Ізраїль).[6]

Незважаючи на те, що Україна увійшла до трійки лідерів з DDoS-атак. За даними Лабораторії Касперського, 12% від усіх атак припадає на Україну. Зі зростанням обсягів безготівкових розрахунків зростає й кількість потерпілих від кібершахраїв. За даними НБУ, у 2011 році кількість протиправних операцій за платіжними картами українських банків зросла до 7,6 тис. порівняно 2,9 тис. роком раніше. Обсяг неправомірно списаних коштів збільшився майже в півтора рази - з 6,3 млн до 9,1 млн грн. І це лише офіційна статистика, до того ж за 2011 рік. [7]

Першою причиною розвитку кіберзлочинності, як і будь-якого бізнесу, є прибутковість. Другою причиною зросту кіберзлочинності як бізнесу є те, що вчинення цих злочинів не пов'язана з великим ризиком. [5]

Указані злочини є надзвичайно латентними, мають у собі складність виявлення, здійснення досудового розслідування, доказу в суді подібних справ та досить велику збитковістю навіть від одиничних випадків їх учинення.

В Україні нормативно-правову базу правового регулювання в сфері кіберзлочинності складають Конституція України, Кримінальний кодекс України, Кримінальний процесуальний кодекс України, Конвенція Ради Європи «Про кіберзлочинність», Закони України «Про основи національної безпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо, Укази Президента України від 08 липня 2009 року № 514/2009, від 08 червня 2012 року № 389/2012, № 390/2012, інші нормативно-правові акти.[2,3]

Крім того, на урядовому рівні створено робочі групи, які розробляють проекти законодавчих актів у сфері громадських стосунків стосовно використання інформаційних технологій, які відображають питання боротьби з кіберзлочинністю і взаємодію з різними міжнародними державними та правоохоронними структурами.

Кримінальний кодекс України є правовою основою по протидії комп'ютерної злочинності. В цьому Кодексі окремі види комп'ютерних злочинів (кіберзлочинів) виділено в Розділ VI Особливої частини - це злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж (ст. 361, 361, 363). У Розділі V

зазначено окремі види злочинів, в яких комп'ютерні продукти визначено як засіб злочину (ст. 163, 176, 177) та злочини у сфері господарської діяльності (ст. 200) в Розділі УЛ.[8]

Служба безпеки України і Міністерство внутрішніх справ України в особі Управління боротьби з кіберзлочинністю опинилися на вістрі війни з «кіберами». На жаль, їхніх зусиль замало,особливо, зважаючи на українські реалії. Наша країна з її низьким рівнем обізнаності про загрози використання комп'ютерів і низьким рівнем інформаційної безпеки стає для них справжнім клондайком. Розкрадання коштів в системах Інтернету банкінгу, даних кредитних карт, DDoSатакі на сайти, шахрайство в інформаційних мережах і інсайдерські витоки інформації стають повсякденними явищами.

Лише після ратифікації Україною Конвенції про кіберзлочинність від 7 вересня 2005 року вважається за доцільне вживати термін кіберзлочини, [4]однак до цього часу немає чіткого визначення цього терміну.

Нами пропонується авторське визначення терміну кіберзлочинності. Отже кіберзлочинність - це сукупність кіберзлочинів, як суспільно небезпечних, винних діянь, учинених у кіберпросторі, за вчинення яких передбачена кримінальна відповідальність.

На нашу думку одним із проблемних питань на сьогодні є затягування досудового розслідування кіберзлочинів,у зв'язку з малою кількістю досвідчених державних експертів в області комп'ютерно-технічної експертизи,та, складнощами з уведенням у правове поле досліджень фахівців комерційних організацій. Типовий термін проведення комп'ютерно - технічних експертиз становить від півроку і більше через високу завантаженість профільних державних установ, а підозрюваний може утримуватися в слідчих ізоляторах весь цей час.

Крім того, мусимо констатувати, що й законодавство України є недосконалим у сфері боротьби з кіберзлочинністю. Так, відповідно до п. 7 ч. 1 ст. 162 КПК України до охоронюваної законом таємниці, яка міститься в речах і документах, належить інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо. [9] Для отримання доступу до речей і документів, визначених у зазначеній статті, згідно зч. 1 ст. 160 КПК України, слідчому за погодженням з прокурором необхідно звернутися з відповідним клопотанням до слідчого судді. [9]

На нашу думку, технічна інформація щодо IP-адреси, MAC-адреси пристрою та публічні послуги не є персональними даними, її розголошення правоохоронними органами не порушує право людини на приватність спілкування оскільки зміст повідомлень не розкривається. Наявність зв'язку між абонентами також не є охоронюваною інформацією, а оператори та провайдери телекомунікацій надають публічні послуги, які не є інформацією з обмеженим доступом крім розкриття персональних даних абонента (ст. 31 Конституції України [1]).

З метою врегулювання цієї ситуації доцільно було б п. 7 ч. 1 ст. 162 КПК України викласти в такій редакції:«інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зміст сигналів, що передаються в комп'ютерних мережах електрозв'язку».

Кіберзлочинність - це проблема, з якою зіштовхнулась планета у XXI столітті, і яка зростає незважаючи на заходи попередження та реагування. У деяких міжнародних документах визначено, що кіберзлочинність загрожує не тільки національній безпеці окремих держав, а й міжнародному порядку. Стурбованість міжнародного співтовариства щодо розвитку кіберзлочинності знайшла відображення в Бангкокській декларації з попередження злочинності та кримінального правосуддя (2005 року), Бухарестській декларації про міжнародне співробітництво в боротьбі з тероризмом, корупцією і транснаціональною організованою злочинністю (2006 року), Всесвітньому саміті з інформаційного суспільства та Конвенції Ради Європи «Про кіберзлочинність» (2001 року). У цих документах йдеться мова про спільне протистояння кіберзлочинцям, шляхом прийняття відповідних законодавчих актів, які не будуть суперечити ні законам окремої держави ні пунктам договорів, які ратифікувала ця держава. Жодна держава не в змозі протистояти кіберзлочинності самостійно, тому сьогодні є необхідність активізації міжнародної співпраці в цій сфері.

Таким чином, пропонується державним органам по боротьбі з кіберзлочинністю переглянути всі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців,запроваджувати сучасні новітні інформаційні технологій, в органах державної влади вносити пропозиції щодо перепідготовки та підвищення кваліфікації фахівців. Не зволікаючи здійснювати реорганізацію,удосконалення законодавчої й нормативно-правової бази та сприяти створенню взаємодії по боротьбі з кіберзлочинністю із зарубіжними законодавчими органами.

Список використаних джерел

1. Конституція України від 28.06.1996 № 254к/96-ВР // Відомості Верховної Ради України (ВВР). - 1996.

2. Про основи національної безпеки: Закон України від 19.06.2003 № 964-IV (із змінами та доповненнями) // Відомості Верховної Ради України (ВВР), 2003, № 39, ст.351

3. Про судову експертизу: Закон України 25.02.1994 № 4038-XII (із змінами та доповненнями) // Відомості Верховної Ради України (ВВР), 1994, N 28, ст.232

4. Про ратифікацію Конвенції про кіберзлочинність»: Закон України від 7 вересня 2005 року N 2824-IV. // [Електронний ресурс]. - Режим доступу: http: //zakon4 .rada.gov.ua/laws/show/2824-15.

5. Голубев В.А. «Кибертерроризм»- миф или реальность? Центр дослідження комп'ютерної злочинності.

6. Каррыев Б.С., Айдарханов М.Б., Балафанов Е.К. Электронное учебное пособие: Основы информационной культуры, Алмата, IFAP, 2005
7. Всеукраїнська правова газета «Правосуддя в Україні» Режим доступу : http: //ukrj ustice.com.ua/pravove-rehulyuvannya-kiberzlochynnosti/
8. Кримінальний кодекс України / [Електронний ресурс] - Режим доступу: http: //zakon4 .rada.gov.ua/laws/show/2341-14
9. Кримінальний процесуальний кодекс України/ [Електронний ресурс] - Режим доступу: http://zakon4.rada.gov.ua/laws/show/4651-17

Турова Є.О., студентка юридично-психологічного факультету НАВС *Науковий керівник:* Катеринчук К.В., кандидат юридичних наук, доцент

Міжнародий досвід відповідальності за злочини, вчинені внаслідок провокації

На сьогодні в судовій практиці у кримінальних справах часто трапляються такі ситуації, коли вчинення людиною злочину спровоковано працівниками міліції або інших правоохоронних органів. Як правило, такі ситуації виникають по справах про такі злочини, як дача або одержання хабара, по справах, пов'язаних з незаконним обігом наркотичних засобів. Слід зазначити, що Європейський суд з прав людини (далі ЄСПЛ) виключає відповідальність особи за злочини, вчинені внаслідок провокацій зі сторони працівників правоохоронних органів. У свою чергу, відповідно до українського законодавства, рішення ЄСПЛ є для українських судів джерелом права й підлягають застосуванню для правовідносин, що виникають у судовій практиці. Проте невідому чому, але вітчизняні суди посилаються на правові позиції, викладені в постановах Пленуму Верховного Суду, які не є керівними.

Сьогодні можна спостерігати ситуацію, коли органи внутрішніх справ вчиняють дії, які можна розцінювати як провокацію, а стаття 271 Кримінально-процесуального кодексу України, яка називається «Контроль за вчиненням злочину» [1, ст.271] не в повній мірі відповідає практиці Європейського суду. Оскільки не зовсім чітко враховано питання провокації в національному законодавстві, то це призводить до того, що ні судді, ні прокурори не дивляться на практику Європейського суду з прав людини та не враховують Конвенцію про захист прав людини та основоположних свобод. Практиці відомі такі випадки, коли правоохоронні органи використали докази отримані внаслідок провокації, вчиненої не працівником міліції, а фізичною особою і судом були прийняті такі докази. Проте ЄСПЛ наголошує, що це порушує вимоги статті 6 Конвенції «Право на справедливий суд» [2, ст.6].