

ухвалою суду» (ст. 79 КПК України). Таким чином, предмет набуває процесуального значення речового доказу після відповідної процедури, що передбачена законом. До цього виявлені або представлені сторонами або сторонніми особами предмети не можуть визнаватися речовими доказами, що має знайти відображення в чинному КПК України. Сторони представляють не процесуальні докази, а предмети, речі, документи, котрі, у встановленому порядку, можуть бути визнані доказами у кримінальному провадженні.

На завершення слід зазначити, що у загальній нормі про слідчий огляд мають бути названі найбільше розповсюджені, за об'єктом обстеження, його види: місця події, місцевості, приміщень, трупа, предметів, документів. Оскільки наведений перелік не може бути вичерпним, а предмети (речі) матеріального світу можуть бути надзвичайно різноманітні, даний перелік закінчити словами «та інших матеріальних об'єктів з метою виявлення слідів кримінального правопорушення, з'ясування інших обставин, що мають значення для кримінального провадження».

Список використаних джерел:

1. Кримінальний процес : підручник / Ю. М. Грошевий, В. Я. Тацій, А. Р. Туманянц та ін.; за ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. – Х. : Право, 2013.
2. Кримінальний процесуальний кодекс України. Науково-практичний коментар / За загальною редакцією професорів В. Г. Гончаренка, В. Т. Нора, М. Є. Шумила. – К. : Юстініан, 2012.

Кіберзлочинність: деякі проблеми розслідування та попередження

Топчій В.В., професор кафедри кримінального права, процесу та криміналістики Національного університету Державної податкової служби України, доктор юридичних наук, доцент, заслужений юрист України

У ХХІ 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 заповнили 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, символічному 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.

На відміну від традиційних видів злочинів, кіберзлочинність явище відносно 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 Fraud and Abuse Act», 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 збитковість 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 VII. [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, DDoS-атаки на сайти, шахрайство в інформаційних мережах і інсайдерські витoki 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.

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

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 навантаженість профільних державних установ, а підозрюваний не 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 з ч. 1 ст. 160 КПК України, слідчому за погодженням з прокурором необхідно звернутися з відповідним клопотанням до слідчого судді. Пропонується, що 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 ХХІ 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 самотійно, 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 технології, 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.

Про деякі аспекти державного патерналізму

Осадчий М.М., провідний науковий співробітник відділу організації науково-дослідної роботи НАВС, заслужений юрист України

Євроінтеграційні прагнення України, офіційно започаткований процес удосконалення Конституції України та проведення всеохоплюючих економічних реформ – основні причини, які змушують приділити увагу й ще раз замислитися над питанням державного патерналізму.

Не викликає сумніву, що соціальний захист населення є безумовно функцією сучасної держави, проте еволюція цього явища у тому вигляді, що є звичним для нас, нараховує як мінімум століття.

Впродовж всього цього часу громадяни боролись за свої соціальні права, поступово добиваючись від суб'єкта управління збільшення виплат, розробки та реалізації соціальних програм, приймаючи при цьому безпосередню участь в реалізації подібних політичних рішень.

Відправною точкою надання соціальної допомоги населенню у звичному для нас вигляді можна вважати 1601 р., коли в Англії було прийнято закон «Про бідність», який був грамотним управлінським ходом. Цей нормативно-правовий акт дозволив вирішити декілька насущних проблем. Зокрема, в межах реалізації «Закону про бідність» було проведено перепис та аналітичне опрацювання населення, виокремлено нужденні