УДК 343.98

Віталій Анатолійович СВІТЛИЧНИЙ,
викладач кафедри захисту інформації
факультету підготовки фахівців для підрозділів
боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ,
Юрій Миколайович ОНИЩЕНКО,
викладач кафедри захисту інформації
факультету підготовки фахівців для підрозділів
боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

СТАН ТА ОСОБЛИВОСТІ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Під терміном «кіберзлочинність» прийнято мати на увазі будь-який злочин, здійснений за допомогою віртуального простору і комп'ютерів. У реальному світі кібератаки паралізують діяльність серйозних фірм, електронних ЗМІ, громадяни втрачають гроші завдяки різним шахрайським схемам. Проте точний об'єм втрат визначити неможливо, адже багато фірм піклуючись про свою репутацію, не називають суми своїх збитків, а деякі з них навіть не підозрюють, що на них здійснювалися напади з боку кіберзлочинців. Тому недивно, що безпекою кіберпростору стурбовані уряди більшості країн світу.

У МВС України створено Управління по боротьбі з кіберзлочинністю. Основним завданням якого є організаційне і практичне забезпечення реалізації державної політики по попередженню і протидії злочинам і правопорушенням, що здійснюються з використанням інформаційних технологій і телекомунікаційних мереж, а також протидії легалізації доходів, отриманих від таких злочинів і правопорушень [1].

Боротьба з кіберзлочинністю неможлива без глибокого розуміння правових основ щодо використання інформаційних мереж. Саме аналіз взаємозв'язку між технічними характеристиками мережі Internet і обумовленими цими характеристиками правовими і соціальними проблемами, з якими стикаються законодавці і правоохоронні органи усіх країн, є першим кроком до можливого вироблення механізмів адекватного реагування на розвиток і ріст кіберзлочинності.

Нажаль, в Україні на сьогодні відсутнє ефективне законодавство у сфері боротьби з кіберзагрозами і кіберзлочинами. Як відомо, історія законопроекту № 2483 «Проект Закону

про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України» триває близько двох років і в результаті законопроект не ухвалений.

Країні ще належить зіткнутися з проблемою кіберзлочинності повною мірою, але експерти вже зараз розуміють, що потрібний комплексний підхід, а саме: законодавчі заходи, комп'ютерна грамотність користувачів мережі і активне використання систем інформаційної безпеки великими операторами інтернет-транзакций, такими як банки і оператори стільникового зв'язку. За даними Національного центру підтримки електронного урядування в І кварталі 2013 року наша країна займала «почесне» 5-те місце серед країн, на вебресурсах яких, розміщені шкідливі програми. Кількість зафіксованих інтернет-загроз перевищила 47 млн випадків, а зараженню через веб-ресурси в першому кварталі 2013 року піддалися 49 % українських користувачів. З такими показниками Україна зайняла 8-ме місце в списку країн, мешканці яких піддаються найбільшому ризику зараження в Інтернеті [2].

Кіберзлочинці мають великі знання в областях інформаційних технологій і електроніки, і тому протидіяти їм непросто. Як правило, такі протизаконні дії не обмежуються рамками одного міста або однієї країни. І хоча Кримінальний кодекс України передбачає обмеження свободи на строк до 3 років або позбавлення волі на строк до 12 років для тих, хто промишляє інформаційним шахрайством, проте кіберзлочинців це не зупиняє, недосконалість законодавства, величезні гроші при відносно невисокому ризику бути спійманим, – усе це призводить до абсолютної або майже абсолютної безкарності.

Звичайно, є реальні рішення суду, є відшкодування фінансового збитку, але чи варто довіряти офіційній статистиці? Адже багато хто, комерційні і державні структури, вважає за краще не поширювати інформацію про те, що сталося, особливо це стосується випадків просочування даних, оскільки не бажають, щоб конкуренти використали ситуацію у своїх цілях або іншого негативного розголосу.

Найбільшої шкоди кіберзлочини завдають як фінансовому стану, так і діловій репутації, причому шкода репутації перевищує грошові втрати [3]. Сьогодні економічна і політична

репутація є одними з найбільш важливих активів для комерційних і державних структур, і саме на них ґрунтується довіра клієнтів до банків і громадян до уряду країни. Втрати від крадіжки, комп'ютерного злому одноразові, а тінь, кинута на репутацію, може вплинути на розвиток подій в майбутньому.

Список використаних джерел:

1. Управління по боротьбі з кіберзлочинністю [Електронний ресурс]. – Режим доступу: http://cybercrimecenter.info/ru/.

2. Кіберзлочинність по-українськи [Електронний ресурс]. – Режим доступу: http://internetua.com/kiberprestupnost-po-ukrainski/.

3. Репутаційна шкода від кіберзлочинів удвічі перевищує фінансові втрати банків [Електронний ресурс]. – Режим доступу: http://www.cnews.ru/news/top/index.shtml?2013/11/08/548924.

Одержано 07.11.2013

УДК [343.98:004](477)

Ольга Сергіївна ЛУНЬОВА,
ад'юнкт
Харківського національного університету внутрішніх справ

ОКРЕМІ АСПЕКТИ ПРАВОВОГО РЕГУЛЮВАННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ В УКРАЇНІ

На сьогоднішній день кримінальні правопорушення з використанням комп'ютерних і цифрових технологій – це одні з найактуальніших та динамічних суспільно небезпечних посягань. Розвиток науки й технологій у сфері комп'ютеризації та інформатизації зумовили швидке їх поширення та відповідний ріст суспільної небезпеки.

На початку 90-х років в українській науковій літературі з'явилося поняття «кіберпростір» - це новий, різноманітний за своєю топологією, вид семіотичного простору, в якому операції зі знаками здійснюються за допомогою сучасних комп'ютерних технологій, що полегшують та істотно прискорюють розумову діяльність людей.

Виникнення певних умов для розвитку нових суспільних відносин приводить до появи осіб, які намагаються отримати незаконну вигоду за рахунок відсутності їх належної правової регламентації. Так само сталося і з появою кіберпростору. Через короткий проміжок часу українському суспільству стало добре відомо і поняття «кіберзлочинність» – це злочинність, пов'язана як з використанням комп'ютерів, так і з використанням

інформаційних технологій і глобальних мереж. З'явилася проблема: до органів внутрішніх справ зверталися особи із заявами про порушення їх прав, але такі дії зловмисників не були віднесені до злочинів чинним на той час Кримінальним кодексом. Все це в сукупності призвело до негайної потреби прийняття відповідних нормативних актів, що регулюватимуть виниклі суспільні відносини.

Національне законодавство в сфері захисту, застосування та використання комп'ютерних технологій розвивалось поступово, в декілька етапів.

В 1994 році було прийнято Закон України «Про захист інформації в автоматизованих системах», який в 2005 році було викладено в новій редакції «Про захист інформації в інформаційно-телекомунікаційних системах». Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Стаття 2 закону визначає, що об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Закон України «Про основи національної безпеки» від 19.06.2003 у ст. 7 визначив, що на сучасному етапі одними з основних реальних та потенційних загроз національній безпеці України, стабільності в суспільстві, в інформаційній сфері є комп'ютерна злочинність та комп'ютерний тероризм; а у ст. 8 закріплено, що одним з основних напрямів державної політики з питань національної безпеки України в інформаційній сфері є вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну.

Прийнятий у 2001 році Кримінальний кодекс України у розділі XVI вперше передбачив кримінальну відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, фактично легалізувавши кримінальну відповідальність за протиправні діяння в зазначеній сфері.

Особливою рисою кіберзлочинності є її глобальність та міжнародна розповсюдженість, адже найчастіше зловмисники

Актуальні питання розслідування кіберзлочинів: матеріали Всеукр. наук.-практ. конф., м. Харків, 10 груд. 2013 р. / МВС України, Харк. нац. ун-т внутр. справ. – Х. : ХНУВС, 2013. – 272 с.

У збірнику висвітлено погляди науковців та практиків щодо проблем правового, організаційного та кадрового забезпечення протидії кіберзлочинності, кримінально-процесуальних та криміналістичних проблем розслідування кіберзлочинів в Україні та використання інформаційних технологій і технічних засобів під час їх розслідування.

ОБСЄ Організація з безпеки та співробітництва в Європі
Координатор проектів ОБСЄ в Україні

Опубліковано Координатором проектів ОБСЄ в Україні в рамках проекту «Посилення боротьби з торгівлею людьми та кіберзлочинністю в Україні».

Україна, 01030, Київ
вул. Стрілецька, 16
www.osce.org/ukraine

МВС України

Харківський національний університет
внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Матеріали
Міжнародної науково-практичної конференції

м. Харків, 10 грудня 2013 р.

Харків 2013

Актуальні питання розслідування
А43 кіберзлочинів : матеріали Всеукр. наук.-практ. конф., м. Харків, 10 груд. 2013 р. / МВС України, Харк. нац. ун-т внутр. справ. – Х. : ХНУВС, 2013. – 272 с.

У збірнику висвітлено погляди науковців та практиків щодо проблем правового, організаційного та кадрового забезпечення протидії кіберзлочинності, кримінально-процесуальних та криміналістичних проблем розслідування кіберзлочинів в Україні та використання інформаційних технологій і технічних засобів під час їх розслідування.

УДК 343.98:[343.3/.7:004](477)(063)
ББК 67.9(4УКР)623.19я431

Наукове видання

АКТУАЛЬНІ ПИТАННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Матеріали
Міжнародної науково-практичної конференції

м. Харків, 10 грудня 2013 р.

Комп'ютерне верстання *Білоуса П. О., Зозулі А. О.*

Формат 60х84/16. Ум.-друк. арк. 15,87. Обл.-вид. арк. 13,72.
Тираж 200 пр. Зам. № 2013-24.

Видавець –
Харківський національний університет внутрішніх справ,
просп. 50-річчя СРСР, 27, м. Харків, 61080.
Свідоцтво суб'єкта видавничої справи ДК № 3087 від 22.01.2008.

Надруковано в ТОВ «Компанія "ВАІТЕ"»,
вул. Саперне поле, 26, кв. 27, м. Київ, 01042,
тел. (044) 531-14-32