Література

1. Вехов В.Б. Расследование компьютерных преступлений в странах СНГ : [монография] / В.Б. Вехов, В.А. Голубев; подред. Б.П. Смагоринского. – Волгоград : ВА МВД России, 2004. – 304 с.

2. Голубев В.А. Проблемы борьбы с преступлениями в сфере использования компьютерных технологий : [учеб. пособие] / Голубев В.А., Гавловский В.Д., Цимбалюк В.С. ; под общ. ред. Р.А. Калюжного. – Запорожье: ЗИГМУ, 2002. – 292 с.

3. Бутузов В.М. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток : [наук.-практ.посіб.] / В.М. Бутузов, В.Д. Гавловський, К.В. Тітунина, В.П. Шеломенцев ; за ред. І.В. Бондаренка. – К. : Вид. дім "Аванпост-Прим", 2009. – 182 с.

4. Романюк Б.В. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологий: [наук.-практ.посіб.] / Б.В. Романюк, В.Д. Гавловський, М.В. Гуцалюк, В.М. Бутузов ; за заг. ред. Я.Ю. Кондратьєва. – К. : Вид. ПАЛИВОДА А. В., 2004. – 144 с.

5. Интернет-бизнес и электронная коммерция [Текст]: учебное пособие / А.Э. Калинина. – Волгоград: ВолГу, 2004. – 148 с.

6. DKWLabs Ввод/вывод денежных средств с использованием электронных платежных систем [Электронный ресурс]. - Режим доступа: http://www.dkws.org.ua

7. Департамент Кіберполіції України. Питання фішингу -[Електронний ресурс]. - Режим доступу: https://www.cybercrime.gov.ua/16-novosti/109-yak-uberegtisya-vid-fishingu#news.

8. Незалежна асоціація банків України Ваш захисник від кіберзлочинності [Електронний ресурс]. - Режим доступу: http://anticyber.com.ua/article_detail.php?id=547.

МОТИВИ ТА ЦІЛІ ЗЛОЧИНІВ, УЧИНЕНИХ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Іщук Б.М.
курсант 3-го курсу факультету № 3
Одеського державного університету внутрішніх справ

Ісмайлов К.Ю.
кандидат юридичних наук, майор поліції
завідувач кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

В сучасних умовах відбувається формування єдиного інформаційного простору і злочини у сфері високих технологій стали дуже популярними. У зв'язку з цим, дослідження злочинів у сфері використання комп'ютерів набувають дуже важливого значення, а саме для захисту інформаційної безпеки держави.

Експертна комісія Інтерполу оголосила статистичні результати дослідження співвідношення різних мотивів при вчиненні комп'ютерних злочинів, а саме, що корисливі

мотиви присутні в 66 % випадків, політичні – в 17 %, дослідницький інтерес превалював у 7 % випадків, хуліганство – 5 %, помста – 4 % [2].

Великої суспільної небезпеки набули злочини в кіберпросторі, а саме пов'язані, зокрема з незаконним втручанням у роботу систем і комп'ютерних мереж, розкраданням і несанкціонованою зміною даних. До її характеристик належать: транснаціональність, масштабність наслідків, латентність, анонімність, динамічність темпів зростання та трансформацій, анонімність тощо.

Питанням вивчення різних особливостей даних злочинів досліджували такі науковці, як: Вехов В.Б., Крилов В.В., Мотлях О.І., Салтевський М.В., Хараберюш І.Ф., Шеломенцев В.П. та ін.

Перш ніж розглядати суб'єктивну сторону вчинення злочинів у сфері високих технологій, потрібно визначити, що саме вчені та практики вкладують в поняття кіберзлочину.

Головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України Шеломенцев В.П. у своїй науковій роботі зазначає поняття кіберзлочину : «Відповідно до Конвенції про кіберзлочинність та Додаткового протоколу до неї кіберзлочини у загальному розумінні – це злочини, зумовлені соціальними, технічними та правовими чинниками та пов'язані саме з комп'ютерними системами, тобто із сукупністю пристроїв,один чи більше у відповідності до певної програми виконують автоматичну обробку даних» [1].

На думку професора Дзюндзюка В.Б. «Кіберзлочинність – це діяльність в модельованому за допомогою комп'ютера інформаційному просторі, в якому знаходяться відомості про осіб, предмети, події, факти, явища, процеси представлені в математичному, символьному або будь-якому іншому вигляді і що знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, пов'язана з вчиненням незаконних дій, які полягають в отриманні конфіденційної інформації, незаконному використанні чужих платіжних карт через Інтернет мережу, викрадення конфіденційної інформації, підміна або фальсифікація стратегічно важливої інформації, створенні та розповсюдженні вірусів та шкідливого програмного забезпечення тощо» [9].

Я вважаю, що обидва поняття досить чітко формулюють визначення кіберзлочинності, але більш розгорнуту характеристику надав професор Дзюндзюк В.Б.

Як і в усіх загально визначених злочинах слідчий під час розслідування повинен встановити мотив вчинення злочину. Злочини вчинені в кіберпросторі відрізняються, перш за все, певними складнощами, які полягають в тому, що мотивація кіберзлочинців формується відразу в двох просторах: реальному та віртуальному. При цьому на формування мотивації впливає, як один та і інший простір.

Так, доцент Манжай О.В. зазначає, що мотивами вчинення комп'ютерних злочинів можуть виступати наступні: з корисливих міркувань; хуліганські цілі; з метою приховати інший злочин; внаслідок збігу тяжких особистих чи сімейних обставин; під впливом погрози чи примусу, матеріальної чи службової залежності від злочинця; через політичні інтереси; через помсту; з метою усунення конкуренту (знищення його ділової, соціальної, політичної репутації); задля інтересу; заволодіння результатами наукових досліджень; отримання конфіденційної інформації; для того, щоб вийти з фінансових утруднень; виразити себе, проявити своє "я"; довести свою перевагу над комп'ютерами [7].

Окрім мотивів, також визначають цілі вчинення злочинів, потрібно враховувати, що цілі і мотив – це різні речі. Цілі – це ті пріоритети, які ставить перед собою людина і намагається досягти, коли вона починає свою діяльність, заради досягнення певної мети і результатів, коли ж мотив означає - внутрішні переконання , чому саме людина вчиняє ті чи інші дії.

Якщо розглядати цілі вчинення злочинів у сфері комп'ютерних технологій, до них відносять наступні:

- незаконне отримання грошей, цінних паперів, кредиту, матеріальних цінностей, товарів, послуг, привілеїв, пільг, квот, нерухомості, паливно-сировинних та енергетичних ресурсів, стратегічного сировини; ухилення від сплати податків, платежів, зборів і т. п.;
- легалізація (відмивання) злочинних доходів;
- підробка або виготовлення підроблених документів, штампів, печаток, бланків, грошових білетів в корисливих цілях;
- отримання конфіденційної інформації в корисливих або політичних цілях;
- помста на грунті особистих неприязних відносин з адміністрацією або товаришами по роботі; - дезорганізація валютної системи країни в корисливих або політичних цілях;
- дестабілізація обстановки в країні, територіально-адміністративному утворенні, населеному пункті (у політичних цілях);
- дезорганізація роботи установи, підприємства або системи з метою вимагання, усунення конкурента або в політичних цілях;
- прагнення приховати інший злочин;
- демонстрація особистих інтелектуальних здібностей або переваги [5].

Якщо брати до уваги мотивації злочинців, то кіберзлочини можна поділити на наступні категорії:

1. кібершахрайство з метою заволодіння коштами;
2. кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу);
3. втручання в роботу інформаційних системи з метою одержання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення збитків конкурентам);
4. інші злочини [6; 9].

Список ключових спеціальностей в світі комп`ютерної злочинності відкривають програмісти, які розробляють шкідливі програмні рішення. За ними йдуть торговці краденою інформацією та технічні фахівці, що підтримують IT-інфраструктуру банд. Вище за них в ієрархії стоять хакери, що займаються пошуком вразливих місць, шахраї, які впроваджують фішингові схеми та поширюють спам, та провайдери, які забезпечують хостинг сайтів і серверів злочинців. Вгорі цього списку знаходяться фінансисти, чиї функції зводяться до контролю над надходженням засобів, переміщенням їх з одного рахунку на іншій та відмивання злочинних доходів. А на її верхівці розташовуються лідери злочинних угруповань, які займаються комплектуванням банд і визначенням цілей [8].

Для поліпшення ситуації необхідно проводити такі заходи:

1. сформувати реєстр фахівців з боротьби з кіберзлочинністю з-поміж управлінського апарату, науково-педагогічного складу, практичних працівників, випускників, що пройшли відповідну підготовку;

2. за підсумками роботи міжвідомчого науково-практичного заходу,

3. куди необхідно притягнути провідних фахівців, має бути сформована робоча група з удосконалення державної стратегії боротьби з кіберзлочинністю;

4. має бути прийняте управлінське рішення про системний розподіл підготовки фахівців з цього напряму в конкретних ВНЗ за конкретними спеціалізаціями для слідчих, оперативних і експертних підрозділів;

5. необхідно або усунути дублювання в роботі оперативних підрозділів по боротьбі з кіберзлочинністю, або чітко встановити їх спеціалізацію;

6. в ідеалі має бути створене самостійне Центральне Управління по боротьбі з кіберзлочинністю в Україні. Зважаючи на специфіку діяльності МВС і СБУ, необхідно налагодити взаємодію між ними на етапах підготовки фахівців і проведення наукових досліджень, а в найближчій перспективі – вийти на рівень систематичного проведення спільних оперативно-тактичних навчань [9; с. 4-5].

Отже, кіберпростір по-різному впливає на мотивацію злочинної поведінки в силу наступних причин: у кіберпросторі відбувається не тільки взаємодія, взаємопроникнення і змішування національних культур, але й формування своєї власної культурної середовища - кіберкультури. Саме вивчення впливу кіберкультури на мотивацію кіберзлочинців є важливим завданням для кримінологів, бо вже зараз групи хакерів, скоюють тяжкі злочини, явно виходячи з мотивів, сформованих у кіберсередовищі.

Література

1. Шеломенцев В.П. Щодо використання терміна «комп'ютерні злочини»//Організація протидії злочинам у сфері інтелектуальної власності та комп'ютерних технологій доповіді провідних вчених, представників громадськості, державних службовців та працівників підрозділів ДСБЕЗна міжвідомчому семінарі-нараді. –К., 2009

2. Голубєв, В. Проблемы противодействия киберпреступности и кибертерроризму в Украине. – [січ. 2005 р.].

3. Конвенція про кіберзлочинність від 01.07.2006 р. Та додатковий протокол// Ліга закон [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua

3. Горова С.В. Кіберпрофесіонали та кіберзлочинність//боротьба з організованою злочинністю і корупцією(теорія та практика). -№2(33).-2014

4. Як побороти кіберзлочинність// Віртуальний пресс-центр Майкрософт Україна - 2012 -9 квітня [Електронний ресурс]. – Режим доступу: http://microsoftua.wordpress.com

5. Кіберзлочинність та відмивання коштів [Електронний ресурс]. – Режим доступу: http://www.sdfm.gov.ua

6. Матюшкова Т.П. Окремі версії при розслідуванні комп'ютерних злочинів // Актіальні питання розслідування кіберзлочинів. – Харків. - 2013.

7. Манжай О.В. Структура кіберзлочинності // О.В. Манжай [Електронний ресурс]. – Режим доступу: http://cybercop.in.ua

8. Орлов О.В. Державна політика підготовки кадрів з попередження кіберзлочинності в Україні / О.В. Орлов, Ю.М. Онищенко [Електронний ресурс]. – Режим доступу: http://www.kbuapa.kharkov.ua

9. Дзюндзюк В.Б. Поява і розвиток кіберзлочинності // В.Б. Дзюндзюк, Б.В. Дзюндзюк [Електронний ресурс]. – Режим доступу: http://www.kbuapa.kharkov.ua

ЮРИДИЧНІ ТЕНДЕНЦІЇ ТА КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ В УКРАЇНІ

Музика Л.П.
слухач ННІЗДН факультету №2
Одеського державного університету внутрішніх справ

Ісмайлов К.Ю.
кандидат юридичних наук, майор поліції
завідувач кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

У сучасних умовах активізації інтеграційних та глобалізаційних процесів в Європі та загострення політичної ситуації у відносинах між Україною та Росією все більшої значущості набувають різноманітні аспекти незалежності окремих держав, збереження їх особливої культури, традицій, національних надбань в багатьох сферах соціального буття. У даному контексті проблема юридичного наукового розуміння і практично-правового втілення ідей інформаційного суверенітету набувають підвищеної актуальності. З одного боку, це обумовлено інтенсифікацією процесів обігу інформації у внутрішній та зовнішній сферах соціальних та міждержавних відносин. З іншого – станом юридичної науки та практики, який демонструє невизначеність змісту категорії «інформаційний суверенітет», конфліктність її співвідношення із сучасними юридичними поняттями та явищами «інформаційної свободи» та «інформаційної безпеки» і, водночас, розвитком новітніх категорій: «інформаційної війни» та «інформаційного тероризму».

У наш час тривають дослідження щодо теоретичної розробки категорії суверенітет. Теорія суверенітету збагачується новими поняттями та явищами. Значний обсяг відповідних досліджень має як суто теоретичні висновки, так і практичні результати, що є досить важливим в умовах розбудови України як правової, демократичної та соціальної держави.

Останнє десятиріччя виявило різні, навіть діаметрально-протилежні погляди вчених щодо доцільності введення у правовий обіг цього поняття. Наріжним каменем суперечок у проблематиці інформаційного суверенітету є з'ясування того чи виступає він окремим видом суверенітету, чи повністю підпадає під поняття державного суверенітету.

Виходячи з цього, актуальність наукових досліджень у зазначеній сфері полягає у вирішенні таких питань як виявлення правових джерел походження цієї категорії, визначення поняття, ознак та принципів інформаційного суверенітету, з'ясування його видових та родових зв'язків з іншими явищами та поняттями.

Насамперед, потреба визначити етапи формування, поняття, зміст, правові принципи, механізми правового регулювання відносин у сфері інформаційного суверенітету, перспективи подальшого нормативно-правового врегулювання інформаційно-правових відносин у сучасних умовах становлення інформаційного