Лабунь А.В., Заброда Д.Г., Басиста І.В., Дроздова І.В., Брижик В.О., Мусієнко О.М. – Київ, 2012. – 246с.

9. Гумін О. Зарубіжний досвід запобігання сімейно-побутовим насильницьким злочинам щодо жінок правоохоронними органами / О. Гумін, Г. Римарчук // Вісник Національного університету «Львівська політехніка». – 2016. – С. 502–509.

Торбяк Максим Михайлович,
здобувач ступеня вищої освіти магістра ННІ № 2 Національної академії внутрішніх справ
Науковий керівник: старший викладач кафедри криміналістичного забезпечення та судових експертиз ННІ № 2 Національної академії внутрішніх справ ***Волошин О. Г.***

КІБЕРЗЛОЧИННІСТЬ ЯК СУСПІЛЬНЕ ЯВИЩЕ

Сучасне суспільство – це суспільство інформаційних технологій, що базується на повсякденному використанні комп'ютерної техніки, мереж зв'язку, мобільних засобів комунікації та інших технічних засобів. Щоденна робота урядових структур, банківської, енергетичної, транспортної та інших систем неможлива без надійної роботи комп'ютерної техніки та засобів комунікацій. Інформаційні технології стали постійним супутником сучасної людини не лише на робочому місці, вони увійшли майже в усі сфери людського життя.

На відміну від традиційних видів злочинів, таких як вбивство або крадіжка, історія яких налічує століття, кіберзлочинність явище відносне молоде, яке виникло з появою та розвитком всесвітньої мережі Інтернет.

Під кіберзлочинністю розуміється сукупність злочинів, що вчинюються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних.

Кіберзлочинність – явище новітньої, цифрової доби, тому слід зазначити, що сама природа мережі Інтернет є достатньо сприятливою для вчинення комп'ютерних злочинів. Такі її властивості, як глобальність, трансграничність, анонімність користувачів, охоплення широкої аудиторії, розподіл основних вузлів мережі і їх взаємозамінність створюють кіберзлочинцям, які використовують Інтернет, переваги на всіх етапах вчинення злочину, а також дозволяють ефективно переховуватися від правоохоронних органів.

Оскільки кіберзлочинність невід'ємна від інформаційної революції, то початок її відліку слід вести з шестидесятих років минулого століття. У 1962 році професор Джон Ліклайдер, опублікував свою концепцію широко розповсюдженої комп'ютерної мережі «Galactic Network».

Дана концепція припускала, що в майбутньому з'явиться глобальна мережа, підключитися до якої зможе будь-який охочий, і що дана мережа з'єднає комп'ютерні системи по всьому світу. Що на даний момент уже стало реальністю. Вже у 1970-х роках з'являються перші комп'ютерні злочинці, яких почали називати «хакерами». В більшості літературних джерел як перший професійний кіберзлочинець згадується Джон Дрейпер, який започаткував першу спеціалізацію хакерів, – фрікери, скорочене від «телефонний хакер». В рядах фрікерів у той час були навіть такі відомі особи, як Стів Возняк та Стів Джобс, які в майбутньому заснували «Apple Computers». Вони налагодили виробництво пристроїв для зламу телефонних мереж в домашніх умовах. І саме цей час можна вважати початком розвитку кіберзлочинності.

У 1983 році в США в штаті Мілуокі відбувся перший арешт інтернет-злочинця, про якого стало відомо громадськості. Приводом для цього послужив перший зареєстрований інтернет-злом, здійснений шістьма підлітками, які називали себе «група 414» (414 – міжміський телефонний код Мілуокі). Протягом дев'яти днів ними було зломано 60 комп'ютерів.

У 1984 році Фред Коен опублікував відомості про розробку перших шкідливих комп'ютерних програм, які саморозмножуються, і застосував до них термін «комп'ютерний вірус». При цьому він написав програму, що демонструвала можливість зараження одного комп'ютера іншим.

У 1986 році в США прийнятий перший комп'ютерний закон «The Computer Fraud and Abuse Act», який забороняв неавторизований доступ до будь-якої комп'ютерної системи. Згодом у 1994 році світова спільнота дізналася про так звану «справу Владимира Льовіна», віднесену міжнародною кримінальною поліцією до категорії «транснаціональних мережевих комп'ютерних злочинів». Міжнародна організована злочинна група у складі 12 людей, використовуючи Інтернет, спробувала здійснити 40 переказів грошових коштів на загальну суму 10 млн. 700 тис. 952 долари США з рахунків клієнтів банку, що знаходилися в 9 країнах світу, на рахунки, розташовані в США, Фінляндії, Ізраїлі, Швейцарії, Німеччині, Росії і Нідерландах. Це був перший великий міжнародний фінансовий злочин з використанням Інтернет, про який стало відомо широкій громадськості.

Поява кіберзлочинності і гучні справи про злочинну діяльність міжнародних угруповань, свідчать про те, що в цей час

кіберзлочинність набула таку властивість, як транснаціональність. Так, в 1997 році помилка співробітника «Network solutions» привела до того, що сайти, чиї назви закінчувалися на «.net» і «.com» стали недоступними. Тобто збій в роботі всієї Глобальної мережі відбувся через неуважність всього однієї людини. У цей же час кібератаки стають також способом досягнення політичних цілей: в Інтернеті розповсюджувалися історії про небезпеки і жахи війни, наводилися різні факти і думки політиків і громадських діячів, здійснюючи таким чином пропагандистський вплив на широку аудиторію у всьому світі [8].

В даний час практично будь-який військовий або політичний конфлікт супроводжується організованим протиборством в мережі Інтернет. Для досягнення своїх політичних цілей все частіше стали використовуватися методи інформаційної війни.

Таким чином, на теперішній момент можна виділити 4 етапи в розвитку кіберзлочинності:

1 етап. Поява кіберзлочинності і субкультури хакерів.

2 етап. Розповсюдження кіберзлочинності, поява спеціалізацій кіберзлочинності і національних груп хакерів.

3 етап. Набуття транснаціонального характеру у всіх сферах кіберзлочинності.

4 етап. Використання Інтернету в політичних цілях, виникнення таких явищ, як Інтернет-страйк та Інтернет-війна, цілеспрямоване використання кібератак проти урядів окремих держав.

У листопаді 2001 року країнами Європейського союзу була ратифікована Конвенцією Ради Європи про кіберзлочинність, в якій виділяються наступні групи кіберзлочинів:

1) злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему);

2) злочини, пов'язані з використанням комп'ютера як засобу вчинення злочинів, а саме – для маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерні підроблення);

3) злочини, пов'язані з контентом (змістом даних);

4) злочини, пов'язані з порушенням авторського права і суміжних прав;

5) акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж.

Таким чином, кіберзлочинність є порівняно новим видом суспільно небезпечних діянь, проте на відміну від традиційних крадіжок і шахрайства, вона постійно удосконалюється і йде в ногу з технологіями, що у свою чергу ускладнює виявлення та протидію зазначеним протиправним діям. Ефективний контроль за кіберзлочинністю вимагає більш інтенсивного міжнародного

співробітництва, ніж існуючі заходи по боротьбі з будь-якими іншими формами транснаціональної злочинності.

Для нашої держави досягнення науково-технічного прогресу в галузі високих технологій за останні роки зумовили не тільки стрімкий розвиток і запровадження комп'ютерних систем та мережу у всі сфери людської діяльності, але й появу та поширення нової категорії злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Список використаних джерел

1. Україна увійшла в ТОП-50 країн за рівнем електронної участі громадян в управлінні державою // URL: http://glavcom.ua/news/ukrajina-uviyshla-v-top-50-krajin-za-.
2. Кримінальний кодекс України : Закон від 05.04.2001 р. № 2341 III // Офіційний сайт Верховної Ради України. // URL: //zakon2. rada.gov.ua/laws/show/2341-14/page10
3. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента від 15.03.2016 р. № 96/2016 // URL : http://zakon0.rada.gov.ua/laws/show/96/2016.
4. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні: Наказ МВС України від 07.07.2017 № 575 // URL: http://search.ligazakon.ua/ l_doc2.nsf/link1/RE30805.html.
5. Janika Merilo: Короткий аудит або що зроблено у Львові за рік? Огляд матеріалів ЗМІ «Стратегія - 2020»: інформаційні технології в державному управлінні 20-28 лютого 2015 1 - 31 серпня 2016 року Блоги та соціальні мережі // URL: https://www.facebook.com/ jaanika.merilo?fref=ts.
6. Електронний ресурс // URL: https://www.unian.net/politics/1864456-v-kongresse-ssha-predstavlen-proektzakona-ob-usilenii-kiberbezopasnosti-ukrainyi.html
7. Поняття та кримінологічна характеристика кіберзлочинності // URL: http://libnet.com/content/9684_Ponyattya_ta_kriminologichna_ harakteristika_kiberzloch innosti.html.
8. Поява і розвиток кіберзлочинності // URL: http://www.kbuapa.kharkov.ua/e-book/db/2013-1/doc/1/01.pdf