рядовий міліції, курсант 3-го курсу факультету підготовки кадрів по боротьбі з економічною злочинністю навчально-наукового інституту підготовки кадрів кримінальної міліції НАВС
Никифорчук Вадим Дмитрович
Науковий керівник: кандидат юридичних наук, викладач кафедри оперативно-розшукової діяльності НАВС **Лизогубенко Є.В.**

Поняття кіберзлочинність є поки незвичним для правоохоронних органів, однак злочинні дії для вчинення яких використовується глобальна комп'ютерна мережа Internet, мають велику суспільну небезпеку. Сьогодні значну частину з загального обсягу злочинів починає займати злочинність пов'язана з використанням комп'ютерних систем і мереж. Її зростанню і розвитку сприяє сама природа даного виду злочину, що базується на відкритому і загальнодоступному характері мережі Internet, і безкарності правопорушників, пов'язаної з питаннями юрисдикції, а також недостатньою підготовкою правоохоронних органів з питань розкриття та розслідування таких злочинів.

Національна інфраструктура будь-якої держави вже сьогодні тісно пов'язана з використанням сучасних комп'ютерних технологій. Щоденна діяльність банківських та енергетичних систем, керування повітряним рухом, транспортна мережа, навіть швидка медична допомога перебувають у повній залежності від надійної і безпечної роботи автоматизованих електронно-обчислювальних систем.

Основною метою кіберзлочинця є комп'ютерна система, яка управляє різноманітними процесами, та інформація, що циркулює в них. На відміну від звичайного злочинця, що діє в реальному світі, кіберзлочинець не використовує традиційну зброю – ніж чи пістолет. Його арсенал – інформаційна зброя, всі інструменти, які використовуються для проникнення у мережі, злому і модифікації програмного забезпечення, несанкціонованого одержання інформації або блокування роботи комп'ютерних систем. До зброї кіберзлочинця можна віднести: комп'ютерні віруси, програмні

закладки, різноманітні види атак, які роблять можливим несанкціонований доступ до комп'ютерної системи. В арсеналі сучасних комп'ютерних злочинців є не тільки традиційні засоби, а й найсучасніше інформаційна зброя та обладнання; ця проблема вже давно перетнула кордони держав і отримала міжнародне значення.

Особливу актуальність проблема кіберзлочинності набула в наш час. Соціологічні опитування в різних країнах, і в першу чергу у високорозвинених, показують, що кіберзлочинність посідає одне з чільних місць серед тих проблем, які турбують людей. Більш того, на думку фахівців, сьогодні це явище становить значно серйозну небезпеку, у зв'язку з використанням злочинцями новітніх інформаційних технологій, а також через зростаючу уразливість сучасного індустріального суспільства. Незважаючи на зусилля держав, які направлені на боротьбу з кіберзлочинцями, їх кількість у світі не зменшується, а навпаки, постійно зростає.

Жодна держава сьогодні не здатна протистояти цьому злу самостійно. Нагальною є потреба активізації міжнародного співробітництва, для якого є актуальним, зокрема, налагодження міжнародно-правового механізму регулювання. Але, з огляду на те, що в сучасних умовах значна частина засобів боротьби з кіберзлочинами, як і з іншими злочинами міжнародного характеру, належить до внутрішньої компетенції кожної окремої держави, необхідно паралельно розвивати й національне законодавство, спрямоване на боротьбу з комп'ютерними злочинами, узгоджуючи його з міжнародними нормами права та спираючись на існуючий позитивний досвід.

Статистика говорить сама за себе:

• 86% атакованих хакерами комп'ютерів - домашні;

• Спам становить 54% контрольованого трафіку електронної пошти в світі, в Україну - 82% трафіку;

• Зростання фішингових (пов'язаних з мережевим шахрайством) повідомлень на червень 2011 року склала 81%;

• 18% знешкоджених зразків шкідливих вірусів-нові;

• 4,2 млн. сайтів - порнографічні;

• 55% блогерів пишуть свої Інтернет-щоденники під псевдонімом, побоюючись негативних наслідків у реальному житті;

Мабуть, найбільш вразливими для потоку інформаційного сміття з Всесвітньої мережі є діти. Дослідження показали, що 90%

дітей стикалися в Інтернеті з порнографією, а 65% шукали її цілеспрямовано. Інтерес до «полуничкі» призвів до того, що 44% неповнолітніх користувачів Інтернету хоча б раз піддавалися сексуальним домаганням в Мережі. Ці дані не здадуться настільки дивовижними, якщо мати на увазі, що половина дітей виходять в Інтернет без всякого контролю з боку батьків або педагогів. Більш того, як показують опитування, більшість з них настільки довірливі, що готові надати «віртуальному другу» в Інтернеті свої особисті дані (аж до пін-кодів кредиток батьків).

Проблема протидії комп'ютерній злочинності – це комплексна проблема. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. З цією метою необхідно проводити цілеспрямовану роботу по гармонізації і вдосконаленню законодавства, що регулює поширення інформації в телекомунікаційних мережах. Одним з пріоритетним напрямком є також організація взаємодії і координації зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою.

ЗНЯТТЯ ІНФОРМАЦІЇ З КАНАЛІВ ЗВ 'ЯЗКУ: ПРОБЛЕМИ ТЕОРІЇ І ПРАКТИКИ

рядовий міліції, курсант 3-го курсу навчально-наукового інституту підготовки кадрів кримінальної міліції НАВС
Скульська Олена Віталіївна
Науковий керівник: кандидат юридичних наук, старший викладач кафедри оперативно-розшукової діяльності та спеціальної техніки навчально-наукового інституту підготовки кадрів кримінальної міліції НАВС **Шевчук О.Ю.**

Доведено, що у більшості європейських країн до середини 60-х років XX століття основою для зняття інформації з каналів зв'язку було звичаєве право. Лише після того, як Європейський суд з прав людини визнавав чинне законодавство країни з питань зняття інформації таким, що не відповідає вимогам Конвенції із захисту прав людини, парламенти приводили законодавство країни у відповідність вимогам Європейського суду.

Зняття інформації з каналів зв'язку як оперативно-розшуковий захід передбачає контроль і одночасну фіксацію інформації, що передається каналами зв'язку з метою виявлення даних про