ЕТИЧНІ ВИМІРИ ІНТЕЛЕКТУАЛЬНОГО ТЕРОРИЗМУ В СФЕРІ КОМП'ЮТЕРНОІ ІНФОРМАЦІЇ

Вітчизняні та зарубіжні видання та ЗМІ останніх років переповнені різними поняттями, що позначають ті чи інші нові прояви кримінального характеру в інформаційній галузі. Різновиди цих найменувань наступні: «комп'ютерні злочини», «коммунікаційні злочини», «кібербандитизм» та ін.

При цьому, злочинців іменують «хакери», «кракери», «кіберпанки», «бандити на інформаційних магістралях», які реалізують свої злочинні задуми у сфері інформаційних відносин.

Слід зазначити, що інформаційні відносини виникають за наступних обставин: під час формування та використання інформаційних ресурсів на основі створення, збирання, обробки, накопичення, зберігання, пошуку, розповсюдження і надання споживачеві документованої інформації; створення та використанні інформаційних технологій та засобів їх забезпечення; захисту інформації, прав суб'єктів, шо беруть участь у інформаційних процесах та інформатизації.

Інформація може бути конфіденційною, ознайомлення з якою обмежується її власником або відповідно до законодавства, а також-масовою, тобто призначеною для необмеженого кола осіб.

Правовому захисту підлягає будь-яка документована інформація, утілена у форму, шо дозволяє її ідентифікувати.

Однією з причин виникнення комп'ютерної злочинності стало інформаційно-технологічне переозброєння установ і організацій, насичення їх комп'ютерною технікою, програмним забезпеченням, базами даних. Інша причина - це реальна можливість отримання значної економічної вигоди з використанням ЕОМ в результаті протиправних діянь, а також здійснення морального і психологічного пресингу.

Розрізняють такі види злочинів у сфері комп'ютерної інформації:

1.Неправомірний доступ до комп'ютерної інформації.

Даний злочин зі зовнішньої сторони виражається у неправомірному доступі, спричиняючи знищення, блокування, модифікацію або копіювання інформації, порушення роботи ЕОМ або комп'ютерної мережі.

У спеціальній літературі під неправомірним доступом розуміється отримання можливості винною особою на ознайомлення з інформацією або розпорядження нею на свій розсуд, що здійснюється без згоди власника або його уповноваженої особи. Самостійною формою неправомірного доступу є випадки введення в комп'ютерну систему свідомо неправдивої інформації, яка спотворює зміст і спрямованість даного блоку інформації.

2.Створення, використання та поширення шкідливих програм для ЕОМ.

Шкідливі програми – це програми, які або містять віруси, або команди типу: «логічна бомба», «троянський кінь», «асинхронна атака», «люк», або володіють специфічними властивостями, призначеними для виконання неправомірних або навіть злочинних дій, таких як: розкрадання грошей з банківських рахунків, укриття коштів від оподаткування, помсти, хуліганства і т.д. Дані програми володіють здатністю переходити через комунікаційні мережі з однієї системи в іншу, проникати в ЕОМ і розповсюджуватися як вірусне захворювання.

На даний час фахівцями налічується за різними даними від 3 до 12 тис. різних вірусів і кількість їх постійно зростає. Крім шкідливих програм предметом даного злочину є також машинні носії шкідливих програм.

3.Порушення правил експлуатації ЕОМ, системи ЕОМ чи їхньої мережі.

Подібне порушення правил експлуатації може виражатися в трьох формах:

- у недотриманні встановлених правил, що забезпечують безпеку експлуатації (порушення правил електро- та протипожежної безпеки, ігнорування приписань відповідних інструкцій і т.п.);
- у неналежному дотриманні зазначених правил (наприклад, неповному дотриманні параметрів роботи ЕОМ, порушення алгоритму програм);
- у прямому порушенні цих правил, налриклад, у відключенні системи захисту від неправомірного доступу.

Перші дві форми виконуються шляхом бездіяльності, остання - шляхом активних дій. Ще однією формою праволорушення є комп'ютерне піратство, рівень якого в Росії становить 94%, в Німеччині – 50%, У США – 35%. За данимим Асоціації виробників комп'ютерного забезпечення тільки в Європі збитки від піратства оцінюються в 6-8 млрд. доларів щорічно [1, с.193].

У середині 80-х років у науковій літературі з'явився новий термін «комп'ютерний терроризм», який на думку академіка М.М. Моїсеєва розглядається як «могутня та вкрай небезпечна зброя, не менш потужна за своїми наслідками, ніж атомна» [2, с.83]. Найчастіше під ним розуміються комп'ютерні атаки, сплановані для нанесення максимального збитку по життєво важливих об'єктах інформаційної інфраструктури, а також незаконне знищення або руйнування цифровий власності з метою залякування людей [3, с.35].

За розрахунками зарубіжних експертів, тільки елементарне відключення комп'ютерних мереж призвело б до розорення 20% середніх компаній і 33% банків протягом декількох годин, 48% компаній і 50% банків зазнали б краху протягом декількох діб [4, с.3].

У наш час комп'ютерний тероризм став суворою реальністю. Навіть важко підрахувати загальну кількість кібератак, шо відбуваються у світі, тому що в силу різних причин не всі вони стають надбанням гласності. У 1993р. у Лондоні на адресу цілого ряду брокерських контор, банків, фірм надійшли вимоги виплатити по 10-12 млн.ф.ст. відступних якимось зловмисникам, інакше вони погрожували знищити комп'ютерні системи цих організацій. Всі жертви поступилися і перевели гроші на рахунки в офшорних банках, звідки вони зникли в лічені хвилини [5, с.7-8].

Комп'ютерні інциденти все частіше відбуваються і в Росії. Так у 1999р. був зламаний сайт Ради Безпеки Р.Ф., у 2002р. - сайти МВС і уряду Москви. Цілком зрозумілим стає прагнення Microsoft платити премію в 250 тис. д. за виявлення кожного кібертерориста [6, с.103].

Форми роботи терористів в Інтернеті стають все більш витонченими, а саме:

- в результаті розслідування діяльності «Аль-Каїди» після подій 11 вересня 2001 року ФБР виявила приховану передачу інформації через популярні інтернет-сайти, які не потрапляли під моніторинг спецслужб;
- практикується збір грошових коштів терористами. Зокрема, на сайті Іранської республіканської армії є спеціальний розділ, увійшовши на який можна зробити пожертвування за допомогою кредитної карти. Інші організації використовують для цього підставні благодійні фонди;
- існує і такий вид бізнесу, коли терористи виставляють на продаж вироби зі своєю символікою, а також аудіо-та відеозаписи терактів і виступів своїх лідерів. Для цієї мети використовується не менше 40 мов;
- ведеться спецобробка молоді, якій розповідається, наприклад, про героїчну смерть однолітків-шахідів, тобто формуються «кадри» для підготовки нових терористичних вилазок. Усе це говорить про те, що тероризм в глобальній Мережі розвивається динамічно і широкомасштабно. У світовій Павутині вже налічується понад 4,8 тис. сайтів, що належать екстремістським організаціям (у 1998р. їх було всього 12) [7, с.89].

Для ліквідації електронного тероризму потрібна розробка багатьох заходів, починаючи з прийняття адекватного законодавства і закінчуючи рішенням суто технічних питань. Однак поки що закони окремих держав щодо кібертероризму серйозно різняться і погано сумісні.

Головне ж завдання полягає в тому, щоб на міжнародному рівні розробити комплексну програму, яка включатиме в себе всі можливі форми і методи боротьби з комп'ютерними злочинами - юридичні, програмні, технологічні, організаційні, економічні, політичні і т.д. Ці дії принесуть успіх лише в тому випадку, якщо будуть спиратися на систему постійного моніторингу комп'ютерного тероризму на загальнопланетарному та національному рівнях, що стане дійсними реаліями, а не ілюзіями компьютерно-інформаційної свободи.

Література

1. *Крылов В.В. Информационные компьютерные преступления / В.В. Крылов. - М: Изд.гр. ИНФРА, 1997.-285с.*
2. *Моисеев Н.Н. Судьба цивилизации. Путь разума / Н.Н. Моисеев. – М.: Знания, 1998. – С.83.*
3. *Хиртман К.С. Меняющееся обличье терроризма / К.С. Хиртман // Международный терроризм и право. - М.: Знание, 2004.-С.35.*
4. *Нечипоренко О.Н. Мы стали крайне уязвимы / О.Н. Нечипоренко // Труд. - 1 сент. - 2005. – С.3.*
5. *Терроризм / А.В. Соколов, О.М. Степанюк. - СПб.: Наука, 2002. С. 7-8.*
6. *Еляков А.Н. Компьютерный терроризм / А.Н. Еляков // МЭ и МО. - 2008. - № 10. – С.102-105.*
7. *Панорамаа: Дайджест иностранной аналитической информации.- 2007.*

- № 40. – С.89.

Гусєв, В.І. Етичні виміри інтелектуального тероризму в сфері комп'ютерної інформації. / В.І. Гусєв // Реалії та ілюзії свободи: філософський аналіз сучасності: матеріали Всеукраїнської науково-практичної конференції (21-22 жовтня 2011р). – Полтава: ПНПУ ім. В.Г. Короленка, 2011. – С. 63-66