КРИМІНАЛЬНЕ ПРАВО, КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО, КРИМІНОЛОГІЯ

Крочак Т.І.
студент,
Білоцерківський національний аграрний університет

КІБЕРЗЛОЧИННІСТЬ – КРИМІНАЛЬНА ЗАГРОЗА СЬОГОДЕННЯ

Процеси глобалізації, зокрема глобалізації інформаційних технологій, надають необмежені можливості для надання впливу на особистість і суспільство. Одним з негативних наслідків розвитку інформаційних технологій є поява і розвиток нової форми злочинності – злочинність у сфері високих технологій, коли комп'ютери чи комп'ютерні мережі виступають в якості об'єкта злочинних посягань, а також засобу чи способу вчинення злочинів. Проблема кіберзлочинності актуалізувалася в епоху інформаційного суспільства, коли комп'ютери і телекомунікаційні системи охопили всі сфери життєдіяльності людини і держави, а глобальна мережа Інтернет є однією з найбільш швидких областей розвитку телекомунікаційних технологій. Сьогодні жертвами злочинців, які працюють у віртуальному просторі, можуть стати не тільки люди, але й цілі держави. При цьому безпека тисяч користувачів може опинитися в залежності від декількох злочинців.

Кількість злочинів, скоєних у кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж. Так, у 60-х роках XX століття, коли комп'ютерні мережі використовувались в основному у військових і наукових установах, основною небезпекою вважалася втрата секретної інформації, а також несанкціонований доступ до неї. У 70-ті роки на перший план вийшли проблеми економічної злочинності в сфері комп'ютерних технологій – зломи банківських комп'ютерних мереж, промислове шпигунство. У 80-х роках широко поширеними злочинами стали зломи і незаконне розповсюдження комп'ютерних програм. З появою і розвитком в 90-х роках мережі Інтернет з'явився цілий спектр проблем, пов'язаних із злочинними посяганнями на конфіденційність приватної інформації, поширенням в мережах дитячої порнографії, функціонуванням віртуальних мережевих спільнот екстремістської спрямованості [1].

Інтеграція телекомунікаційних мереж і їх конвергенція, поява можливості «мобільного доступу в Інтернет і все більшого вдосконалення пристроїв доступу до мережі, в тому числі мобільних телефонів, створює нові можливості для зловживання інформаційними технологіями. Для більшості злочинів, скоєних в глобальних комп'ютерних мережах, характерні наступні особливості:

1. Підвищена скритність вчинення злочину, забезпечується специфікою мережевого інформаційного простору (розвинені механізми анонімності, складність інфраструктури).

2. Транскордонний характер мережевих злочинів, при якому злочинець, об'єкт злочинного посягання, потерпілий можуть перебувати на територіях різних держав.

3. Особлива підготовленість злочинців, інтелектуальний характер злочинної діяльності.

4. Нестандартність, складність, різноманіття і часте оновлення способів вчинення злочинів і застосовуваних спеціальних засобів.

5. Можливість вчинення злочину в автоматизованому режимі в декількох місцях одночасно. Можливість об'єднувати відносно слабкі ресурси багатьох окремих комп'ютерів в потужне знаряддя вчинення злочину.

6. Багаторазовий характер злочинних дій при множинності потерпілих.

7. Необізнаність потерпілих про те, що вони піддалися злочинному впливу.

8. Дистанційний характер злочинних дій в умовах відсутності фізичного контакту злочинця і потерпілого.

9. Неможливість запобігання та припинення злочинів даного виду традиційними засобами [2].

Термін «кіберзлочинність» в даний час часто вживається поряд з терміном «комп'ютерна злочинність», причому нерідко ці поняття використовуються як синоніми. Так, Оксфордський тлумачний словник визначає слово «cyber-» як компонент складного слова. Її значення – «відноситься до інформаційних технологій, мережі Інтернет, віртуальної реальності» [3].

Практично таке ж визначення дає Кембриджський словник: приставка «cyber-» означає «включає в себе використання комп'ютерів або відноситься до комп'ютерів, особливо до мережі Інтернет». При цьому в якості прикладу Кембриджський словник наводить слово «cybercrime» – кіберзлочинність (кіберзлочин) [4].

Таким чином, «cybercrime» – це злочинність, пов'язана як з використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж. У той же час термін «computer crime» відноситься тільки до злочинів, що вчиняються проти комп'ютерів або

комп'ютерних даних. Багатьма авторами ведеться збір інформації про стан кіберзлочинності. Експерти залишилися одностайні: в даний час не існує ні релевантної статистики, що відбиває реальну картину стану кіберзлочинності, ні надійних методів збору таких даних [5].

Тенденції, відзначені експертами ООН, говорять про зміну структури найбільш поширених посягань, що пов'язано з розвитком телекомунікаційних технологій і ростом кількості користувачів мережі Інтернет. Можна навести десять найбільш небезпечних загроз, що відзначаються фахівцями: мережі ботів; «цілеспрямовані» атаки на урядові сайти, приватні підприємства, та кінцевих користувачів; фінансове шахрайство, потерпілими від якого є банки, приватні підприємства і кінцеві користувачі; шахрайство з посвідченням особи; спам і фішинг; шпигунство – економічний і у державних органах; Web-атаки; соціальні мережі; неправильне або зловмисне використання внутрішніх мережевих ресурсів; віруси і черв'яки [6].

Сьогодні практично всі дослідники та фахівці визнають, що ситуація з кіберзлочинністю поки має тенденцію до погіршення. Ще одна небезпечна тенденція – все більший зв'язок між кіберзлочинністю та організованою злочинністю. Можна з упевненістю сказати, що Інтернет використовується злочинними групами вже не тільки як допоміжний засіб, але і як місце і основний засіб вчинення традиційних злочинів – шахрайств, крадіжок, вимагань.

Чинний Кримінальний процесуальний кодекс не містить положення, які дають змогу використовувати докази в електронній формі. Таким чином, фактично відсутня можливість доказування наявності того чи іншого протиправного діяння, пов'язаного з рухом інформації в електронному вигляді в реальному масштабі часу. Наразі єдиним способом використання електронної інформації як доказів у суді є висновок експерта. Таким чином, доказами у кримінальній справі можуть бути використанні висновки комп'ютерно-технічної експертизи, виконаної відповідно до Закону «Про судову експертизу». Позитивним в цьому аспекті є можливість здійснення експертизи не тільки в державних спеціалізованих установах, а й у незалежних експертів, які атестовані в порядку, визначеному законодавством України.

Слід зазначити, що в Україні Департамент по боротьбі з кіберзлочинністю МВС України було створено у грудні 2011 р., а відповідні територіальні підрозділи почали створюватися лише на початку 2012 р. Проте вітчизняний сучасний стан нормативної бази щодо запобігання та регулювання відносин у сфері кібернетичної злочинності в цілому можна охарактеризувати як недосконалий через наявну безсистемність і відсутність термінологічної визначеності в базових поняттях [7].

Чинне кримінальне законодавство про відповідальність за злочини у сфері комп'ютерної інформації говорить тільки про комп'ютерні злочини, тобто злочини, які вчиняються щодо комп'ютерів і комп'ютерної інформації (злочини проти комп'ютерної безпеки), але не стосується інших злочинів, що здійснюються з їх використанням. В даний час все частіше говориться про необхідність криміналізації спаму. З таким явищем, як спам, можна і потрібно боротися, але його суспільна небезпека – одне з основних підстав для криміналізації діяння, що необхідно передбачати кримінальну відповідальність за вчинення таких дій. Цілком достатньо було б внесення норм про відповідальність за розповсюдження спаму в кодексі про адміністративні правопорушення.

Список використаних джерел:

1. Бондаренко С.В. Виртуальные сетевые сообщества девиантного поведения [Електронний ресурс] / С.В. Бондаренко. – Режим доступу: http://www.cyberpolitics.ru/content/view/256/34/

2. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография / А.Л. Осипенко. – Омск, 2009. – С. 109–110.

3. Oxford English Dictionary [Електронний ресурс]. – Режим доступу: www. askoxford.com/

4. Cambridge Advanced Learner's Dictionary [Електронний ресурс]. – Режим доступу: http://dictionary.cambridge.org

5. Gercke M. Understanding Cybercrime: A Guide for Developing Countries. ITU, 2009.

6. Ifrah L. Cybercrime: current threats and Trends. COE, 2008.

7. Правове регулювання кіберзлочинності [Електронний ресурс]. – Режим доступу: http://ukrjustice.com.ua/pravove-rehulyuvannya-kiberzlochynnosti/

Магдич Б.А.
студент,
Білоцерківський національний аграрний університет

ЗЛОЧИННІСТЬ У США ТА ВЕЛИКОБРИТАНІЇ: СТАН, ТЕНДЕНЦІЇ

Порівняльний аналіз кримінальної політики різних країн є досить молодим напрямком сучасної кримінологічної науки. Використання методології порівняльних досліджень здатне виявити ті чинники, які впливають на характер цієї політики і її ефективність. Однак вивчення форм і методів протидії злочинності неможливо без розуміння стану самої злочинності і її тенденцій. Метою цієї роботи є виявлення основних тенденцій стану злочинності в США і Великобританії на основі