СЕКЦІЯ 3
ПРОБЛЕМИ БЕЗПЕКИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Богдан Грималюк
студент 2 курсу спеціальності 201 «Агрономія»
Науковий керівник: **Мушеник І.М.**
к.е.н., доцент кафедри інформаційних технологій,
Подільський державний аграрно-технічний університет,
м. Кам'янець-Подільський

ОСОБЛИВОСТІ ЗЛОЧИНІВ В СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Перехід індустріального суспільства до інформаційного супроводжувався стрімким розвитком комп'ютерних технологій, безпосередньо впровадженням засобів комп'ютерної техніки до виробництва, торгівлі, а також до життя і побуту людей. Комп'ютерні технології стали найголовнішим засобом обміну інформації, які значно полегшили як життя, так і роботу людей. Але разом із значними перевагами дані технології створюють реальні загрози як для правопорядку в певній країни, так і світового правопорядку, оскільки з'явилися нові можливості для вчинення раніше невідомих правопорушень, які мають свої особливості.

Питанням злочинів у сфері використання комп'ютерних технологій займалися наступні науковці: Д. Азаров, О. Баранов, В. Гавловський, М. Гриців, М. Гуцалюк, М. Карчевський, А. Музика, В. Цимбалюк та ін.

За експертними оцінками, сьогодні у світі доходи в сфері комп'ютерної злочинності посідають третє місце після доходів наркобізнесу та торгівлі зброєю [1, с. 20]. І на сьогодні злочини в сфері використання комп'ютерів це одна із груп суспільно небезпечних діянь, яка динамічно розвивається та набирає обертів.

Взагалі, комп'ютерна злочинність – це особливий вид злочинів, пов'язаних із незаконним використанням сучасних інформаційних технологій і засобів комп'ютерної техніки [2]. В їх основі можуть бути політичні, хуліганські, корисливі й інші мотиви. Згідно із чинним законодавством України, кримінальну відповідальність за злочини у сфері використання електронних обчислювальних машин (ЕОМ), комп'ютерних мереж і мереж електрозв'язку передбачено у Розділі XVI Кримінального кодексу України.

Даний вид злочинів з'явився відносно недавно і має ряд особливостей, які притаманні і характеризують лише їх. Так, необхідно звернути увагу на предмет злочину. Ними будуть: електронно-обчислювальні машини (ЕОМ), автоматизовані комп'ютерні системи (АКС), комп'ютерні мережі, носії комп'ютерної інформації. ЕОМ – комплекс електронних технічних засобів, побудованих на основі мікропроцесорів і призначених для автоматичної обробки інформації при вирішенні обчислювальних та інформаційних завдань. АС – це організаційно-технічні системи, в яких реалізується технологія обробки інформації з використанням технічних і програмних засобів. Зокрема, такими системами слід вважати сукупність ЕОМ, засобів зв'язку та програм, за допомогою яких ведеться документообіг, формуються, оновлюються та використовуються бази даних, накопичується та обробляється інформація. Оскільки обробка певних даних можлива і в результаті роботи одного комп'ютера, то АС – це й окремо взятий комп'ютер разом з його програмним забезпеченням. Комп'ютерна мережа – це сукупність програмних і технічних засобів, за допомогою яких забезпечується можливість доступу з однієї ЕОМ до програмних чи технічних засобів інших ЕОМ та до інформації, що зберігається у системі іншої ЕОМ. Мережа електрозв'язку – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

В свою чергу Сьюзан В. Бренер виокремлює наступні особливості, що відрізняють дані злочини від інших. По-перше, даний вид злочину не вимагає фізичного зближення між жертвою та суб'єктом злочину в момент вчинення злочину. По-друге, вони часто є «автоматизованими». По-третє, суб'єкт даного злочину не підвладний обмеженням, що існують у реальному фізичному світі. По-четверте, наука не здатна ще встановлювати моделі розповсюдження різних видів даних злочинів географічно та демографічно. І останньою особливістю є складність встановлення місця злочину [3, с. 33].

Якщо казати про першу особливість, то увага звертається на те, що суб'єкт та потерпіла особа безпосередньо можуть знаходитися взагалі на різних континентах і це не буде обставиною, яка заважатиме суб'єкту вчинити даний злочин.

Щодо того, що даний вид злочинів – «автоматизовані», то це означає, що суб'єкт злочину за допомогою комп'ютерних технологій і за відносно короткий проміжок часу може підвищити кількість злочинів, які вчиняються.

Однією із особливостей злочинів та найголовніших проблем для правоохоронних органів є встановлення місця вчинення злочину, а також – право якої держави повинно застосовуватися, якщо об'єкт та суб'єкт знаходяться в різних країнах. Питання визначення місця вчинення злочину вирішується по-різному на розсуд національних судів. Необхідно звернути уваги також і на те, суди різних країн світу встановлюють свою територіальну юрисдикцію щодо злочинів з використанням комп'ютерних технологій в залежності від наступних підстав: 1) місце вчинення злочинного діяння; 2) місце знаходження комп'ютеру; 3) місце знаходження осіб (суб'єкт злочину або особа, яка є потерпілим від злочину, знаходиться на території країни) – принцип суб'єктивної територіальності; 4) місце настання суспільно небезпечного наслідку (істотний шкідливий наслідок діяння настає на території країни) – принцип об'єктивної територіальності; 5) місце знаходження будь-якої з перерахованих підстав, в тому числі й транзит інформації через територію країни.

Ще однією особливістю даної групи злочинів є розмежування їх залежно від об’єкта. Тобто, в залежності від того, на що посягається суб’єкт злочину. Так, виділяють злочини, які націлені та спричиняють шкоду конкретним об’єктам (наприклад, викрадення конфіденційної інформації із комп’ютера) та злочини, які націлені та посягають на невизначене коло об’єктів (наприклад, створення та розповсюдження вірусних програм).

Таким чином, злочини із використанням комп’ютерних технологій стають дедалі розповсюдженими, але вони і досі залишаються феноменами, так як наука ще не здатна чітко встановити правове регулювання відповідальності за дані злочини, оскільки вони мають ряд своїх особливостей та технології досить стрімко розвиваються, що і зумовлює появу нових видів злочинів із використанням комп’ютерних технологій.

Список використаних джерел

1. Гавловський В.Д., М.В. Гуцалюк, В.С. Цимбалюк Удосконалення інформаційного законодавства як засіб оптимізації протидії комп’ютерній злочинності // Науковий вісник Національної академії внутрішніх справ України. – 2001. – № 3. – С. 20-24.

2. Судова практика розгляду справ про злочини у сфері використання електроннообчислювальних машин (комп’ютерів), автоматизованих систем та комп’ютерних мереж і мереж електрозв’язку / Верховний Суд України: інформаційний сервер // [Електронний ресурс]. – Режим доступу: Особливості злочинів в сфері використання комп’ютерних технологій[Електронний ресурс] режим доступу - http://www.scourt.gov.ua

3. Brenner S. W. Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement? 30 Rutgers Computer & Tech. L.J. 1 (2004).