Волков Юрій Михайлович,
викладач кафедри
тактико-спеціальної підготовки
Дніпропетровського державного
університету внутрішніх справ

Лукомська Аліна Андріївна
курсант 1 курсу ФПФОДР
Дніпропетровського державного
університету внутрішніх справ

ДЕЯКІ АСПЕКТИ МІЖНАРОДНОЇ ПРОТИДІЇ ЗЛОЧИНАМ, СКОЄНИМ ЗА ДОПОМОГОЮ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Інформація в цілому та знання окремо є визначальними факторами, що впливають на розвиток техніки та технологічних ресурсів людства. Можна навіть зазначити, що вони встановлюють межі технологій, а також можливостей розвитку природи та подальшого розвитку суспільства. Застосування сучасних технологій на базі персональних комп'ютерів, інформаційно-обчислювальних мереж та комп'ютеризованих мереж надало кожній людині можливості доступу до даних, що зберігаються у відповідних базах даних, встановлюючи зв’язки незалежно від часу та адміністративних й державних кордонів абонента. Поруч із перевагами, комп'ютеризація має і деякі негативні наслідки.

Багато науковців розділяють комп’ютерні загрози на два типи:

1. Злочини, які були вчинені за допомогою комп'ютерів - це знищення або зміна даних, програмного та апаратного забезпечення - розкрадання вхідних / вихідних даних, програмного та апаратного забезпечення - економічну інформацію про шпигунство та розголошення, яка є державною.

2. Юридичні дії, котрі реалізовані за допомогою користування комп'ютерів як інструменту досягнення злочинної мети:

- комп’ютерний саботаж; вимагання та шантаж; шахрайство на гроші; шахрайські споживачі, інвестори чи користувачі; інші злочини.

До категорії "правопорушень " входить несанкціоноване використання комп'ютера для спеціальних цілей. На нашу думку, комп’ютерні злочини зазначають небезпечну діяльність чи бездіяльність, які реалізуються за допомогою сучасних інформаційних технологій та засобів обчислювальної техніки для заподіяння збитків майновим або соціальним інтересам держави, підприємств, відомств, організацій, кооперативів, цивільних формувань та людей, а також особисті права. [2, 19]

Поширювання загальних комп'ютерних знань, постійне вдосконалення технічних характеристик та супутнє падіння цін на обладнання, застосування комп'ютерів у всіх професіях, розвиток технологічних мов високого рівня, які

легко може опанувати будь-яка зацікавлена особа, і, як наслідок, постійне зростання користувачів спричиняло збільшення кількості злочинів, пов’язаних із застосуванням комп'ютерної техніки. Тобто зростання кримінальних справ, пов'язаних з комп'ютерними злочинами, спостерігається практично у всіх країнах з розвиненою галуззю.

На думку американських експертів, поточний економічний збиток, заподіяний комп’ютерними злочинами, стоїть зараз на одному рівні з перевагами, отриманими від заподіяння комп'ютерів у практику, а соціальні та моральні втрати взагалі не підлягають оцінці.

Така оцінка здебільшого підвищена, але по фактам можна навести достатньо підстав наприклад на тому, що лише в США економічні збитки, завдані комп’ютерними злочинами у 90-роках, наближалися до 100 мільярдів доларів США. Також слід мати на увазі, що цей вид злочинів має високу затримку: лише 10–15% комп'ютерних правопорушень можуть бути виявлені, оскільки організації, які постраждали від таких злочинів, дають інформацію, оскільки це може пошкодити їх авторитет або спричинити повторні злочини. [1, 101]

Враховуючи приховані правопорушення, загальні матеріальні збитки, які щорічно наносяться економічними комп’ютерними злочинами, на думку німецьких експертів збільшуються. Тенденція до збільшення кількості подібних злочинів залишається і надалі, особливо через появи комп’ютерних мереж. Кількість цих злочинів щороку збільшується на 30-40%.

З часом багато країн світу поступово затверджували законодавчі акти щодо злочинів цієї категорії.

Згідно з кримінальним законодавством Італії комп'ютерний злочин - це правопорушення, скоєне за допомогою комп’ютерних технологій, від персонального до переносних телефонних пристроїв, створених на основі мікросхем. Закони Італії забезпечують урядові організації, фірми, військові цілі, банки, компанії захист від несанкціонованого доступу до комп'ютерних мереж, незаконного використання захищених банківських даних, порушення закону копіювання топографій фішок, які злочинці використовують для отримання кодів кредитних та телефонних карток, банківської діяльності рахунки тощо. В Італії щорічні збитки від комп’ютерних злочинів становлять сто мільйонів доларів. Комп'ютерні злочинці характеризуються використанням програмного забезпечення, яке може автоматично приймати всі алфавітні та фігурні поєднання на основі генератора випадків.

У Франції є повний юридичний арсенал для боротьби з такою категорією злочинів. У 1994 році вони створили бригаду поліції, яка має досвід розкриття та розслідування комп'ютерних злочинів у тісній співпраці зі службами безпеки та громадськими організаціями.

Сектор комп'ютерної злочинності (CCS) Федеральної поліції Австралії (AFP) виконує дві функції:

1) збір розвідувальних даних (оперативних та розшукових) даних про

спеціальні комп'ютерні злочини та їх розслідування

2) надання іншим підрозділам технічної підтримки щодо обстеження комп'ютерів, пов'язаних із злочинами що сприяли їх вчиненню.

Злочини, пов'язані з комп'ютерами, - це порушення, в яких комп'ютер виконує роль предмета чи інструменту злочину. Слід зазначити, що приймання грошей з банку за допомогою комп'ютера як інструменту злочину може слугувати прикладом такого типу.

Оскільки технологія використовується для вчинення більш складних злочинів, правоохоронці та особи, які перебувають у правовій системі, все частіше використовують технічні засоби боротьби зі злочинністю. Щоб забезпечити громадський порядок і захистити людське життя, важливо, щоб галузь кримінальної юстиції використовувала передове програмне забезпечення, системи відстеження тощо.

Сьогодні правоохоронні органи можуть використовувати технологію для виявлення та документування злочинної діяльності, що відбувається в даний момент. Ці технології дозволяють правоохоронцям бути більш ініціативними. Деякі технології виявлення, моніторингу та позиціонування, що сприяють правоохоронним органам, включають: безпілотні летальні апарати, технологію зйомки, сканування номерних знаків, тощо.

Коли поліції потрібен аерофоторозгляд місця події, безпілотники можуть допомогти правоохоронцям безпечно спостерігати територію. Глобальні системи позиціонування (GPS): GPS не тільки допомагає поліцейським потрапляти на місця злочину але й знаходити злочинців. Це також допомагає підрозділам краще керувати поліцейськими силами, оскільки карти розповсюдження поліцейських можуть забезпечити охоплення більшої кількості територій. Інтеграція GPS з іншими поліцейськими системами допомагає зробити дані більш надійними, оскільки служби локації безперешкодно включаються у звітування.

Технологія зйомки: ця технологія виявляє стрілянину та дає поліцейським миттєвий доступ до зйомки карт локації, а також інформації про кількість стрільців і скільки пострілів було зроблено. Сканування номерних знаків: ця технологія дозволяє поліцейським миттєво побачити, чи автомобіль був викрадений, або за наявності ордера на арешт водія.

---

1. Вертузаєв М., Попов А. Запобігання комп'ютерним злочинам та їх розслідування // Право України. 1998. № 1. с.101-103.

2. Голубєв В.О. Комп'ютерні злочини в банківській діяльності. Запоріжжя: ВЦ "Павел", 1997. 118 с.

3. Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп'ютерна злочинність. Навчальний посібник. Київ: Атіка, 2002. 240с.

4. Голубєв В.О., Гавловський В.Д., Цимбалюк В.С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Навчальний посібник. / За заг. ред. д.ю.н., професора Р.А.Калюжного. Запоріжжя: ГУ "ЗІДМУ", 2002. 292с.