несанкціонованого доступу до даних; механізму поширення в мережі шкідливих функцій і т.д.);

– з'ясування причинного зв'язку між використанням конкретних апаратно-програмних засобів обчислювальної мережі та результатами їх застосування.

Таким чином, комп'ютерно-мережева експертиза становить собою окремий підвид судової комп'ютерно-технічної експертизи. Маючи свій об'єкт, предмет та завдання, вона дозволяє виявити порушення в мережі Інтернет, помітити несанкціонованого доступу до даних і визначити його сценарій, зафіксувати механізм поширення в мережі шкідливих функцій. Окрім цього в комплексному застосуванні разом з іншими судовими комп'ютерно-технічними експертизами, вона дає можливість відстежити не лише механізм порушення немайнових прав користувачів, але й дозволяє відстежити саму особу порушника. Отже, комп'ютерно-мережева експертиза є дієвим засобом виявлення порушень прав осіб в Інтернет-просторі, їх попередження та протидії.

Список використаних джерел:

1. Мазниченко Ю. О. Інформаційні технології в експертних дослідженнях : [навч.-практ. посібник] / Ю. О. Мазниченко. – К. : Київський нац. ун-т внутр. справ, 2007. – 152 с.

2. Інтернет джерело http://lagman-join.narod.ru/spy/CNEWS/cisco_attacks.html

КОМП'ЮТЕРНО–ТЕХНІЧНА ЕКСПЕРТИЗА: ПОНЯТТЯ, ПРЕДМЕТ, ОБ'ЄКТИ, ЗАВДАННЯ. ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОГЛЯДУ МІСЦЯ ПОДІЇ ПРИ КОМП'ЮТЕРНИХ ЗЛОЧИНАХ, ПРАВИЛА ВИЛУЧЕННЯ КОМП'ЮТЕРНИХ ЗАСОБІВ ТА ЇХ УПАКУВАННЯ

Шульга Б. С., головний експерт відділу комп'ютерно-технічної експертизи, експертизи відео та звуко- запису лабораторії криміналістичної експертизи Державного науково-дослідного експертно-криміналістичного центру МВС України

Розвиток в Україні сучасних інформаційних технологій, телекомунікаційних систем, комп'ютеризація суспільства в цілому приводять до появи нових проблем, у тому числі й у сфері боротьби зі злочинністю. У цьому плані перед правоохоронними органами постає задача своєчасного виявлення, кваліфікованого розслідування злочинів з використанням комп'ютерних технологій і вживання заходів по усуненню причин і умов, що сприяли їх скоєнню.

Практика показує, що з розвитком комп'ютерних технологій вони проникають в усі сфери життєдіяльності суспільства й у механізмі здійснення злочинів можуть відігравати різноманітну роль. При цьому виділяються три групи злочинів.

Перша група – це злочини в сфері використання електронно-обчислювальних машин, систем і комп'ютерних мереж (розділ 16 – ст. ст. 361-3631 КК України). Вони можуть бути згруповані в такий спосіб:

а) несанкціонований доступ до комп'ютерної інформації,

б) злочини, пов'язані зі зміною інформації, її модифікацією,

в) злочини, спрямовані на навмисне знищення, блокування, приведення в непридатний стан комп'ютерної інформації чи програми, а також розробка, використання або поширення шкідливих програм,

г) злочини, що виражаються в порушенні правил експлуатації комп'ютерної системи чи мережі.

Друга група – злочини, скоєні шляхом використання комп'ютерної системи, як засобу досягнення злочинної мети. Як правило, це злочини, спрямовані на заволодіння грошима або власністю шляхом присвоєння, зловживання службовим становищем чи шахрайства. Тобто, це традиційні злочини, у здійсненні яких з'явився новий засіб.

Третя група – злочини, пов'язані з комп'ютером. Насамперед, до цієї категорії варто віднести:

– злочини, у яких комп'ютер виступає як предмет посягання, як матеріальна цінність (наприклад, крадіжка комп'ютера);

– злочини, у яких комп'ютер відіграє роль допоміжного засобу досягнення зв'язку між співучасниками чи сховища інформації.

У криміналістиці перераховані вище злочини варто називати «злочинами, скоєними з використанням комп'ютерних технологій» або «комп'ютерними злочинами».

Огляд місця події. Після прибуття на місце події слідчо-оперативній групі потрібно вжити заходів по охороні місця події та забезпеченню збереження інформації на комп'ютерах і периферійних запам`ятовуючих пристроях (ПЗП). Для цього необхідно:

– заборонити доступ до комп`ютерної техніки працюючого на об'єкті персоналу;

– персоналу об'єкта заборонити вимикати електропостачання комп`ютерної техніки;

– у випадку, якщо на момент початку огляду місця події, електропостачання об'єкту вимкнено, то до його відновлення потрібно відключити від електромережі всю комп'ютерну техніку, яка знаходиться в приміщенні, що оглядається;

– не робити ніяких маніпуляцій з засобами комп'ютерної техніки, якщо їх результат заздалегідь невідомий;

– при наявності в приміщенні, де знаходиться комп`ютерна техніка, небезпечних речовин, матеріалів або обладнання (електромагнітних, вибухових, токсичних, тощо) видалити їх в інше місце.

Після вживання вказаних вище невідкладних заходів можна приступати до безпосереднього огляду місця події і вилучення речових доказів. При цьому потрібно брати до уваги наступне:

– спроби з боку персоналу пошкодити комп`ютерну техніку з метою знищення інформації, якщо до скоєння злочину причетні працівники цього об`єкту;

– наявність в комп`ютерній техніці спеціальних засобів захисту від несанкціонованого доступу, які, не отримавши у встановлений час спеціальний код, автоматично знищать всю інформацію;

– наявність в комп`ютерній техніці інших засобів захисту від несанкціонованого доступу.

Обшук і виїмка речових доказів. При обшуках і виїмках, пов'язаних з вилученням ЕОМ, носіїв інформації виникає ряд загальних проблем, пов'язаних зі специфікою технічних засобів, що вилучаються. Так, необхідно передбачати заходи безпеки, що здійснюються злочинцями з метою знищення речових доказів.

Завершальним етапом огляду, обшуку або виїмки по справах, пов'язаних з використанням комп'ютерних технологій, є фіксація й вилучення комп'ютерних засобів. При вилученні засобів комп'ютерної техніки необхідно забезпечити суворе дотримання кримінально-процесуального законодавства. Для цього необхідно акцентувати увагу понятих на всіх діях, що проводяться, та їх результатах. При необхідності понятим дають необхідні пояснення, оскільки багатьом учасникам слідчої дії можуть бути незрозумілі маніпуляції, що проводяться.

Всі вилучені системні блоки та інші пристрої повинні бути упаковані й опечатані таким чином, щоб виключити можливість їхнього пошкодження, включення в мережу й розбирання.

Під час перевезення комп'ютерних засобів необхідно виключити їхні механічні ушкодження й взаємодію з хімічно активними речовинами. Варто екранувати від впливу електромагнітних полів як комп'ютерні пристрої, так і магнітні носії інформації. Такий вплив може привести до псування або знищення інформації шляхом розмагнічування. Оскільки комп'ютерні засоби потрапляють на дослідження в експертні установи, особливу увагу варто звернути на огородження вилучених об'єктів від впливу широко використовуваних у цих установах магнітоутримуючих засобів криміналістичної техніки (наприклад, магнітних підйомників, магнітних пензликів для виявлення слідів рук і ін.).

Список використаних джерел:

1. Кримінально-процесуальний кодекс України. – К. : 2001.
2. Криміналістична техніка : навч. посібник / Кол. авторів; За ред. А.В. Кофанова. – К. : «КИЙ». – 2006. – 456 с.
3. Криміналістика (криміналістична техніка) : курс лекцій / К82 П.Д. Біленчук, А.П. Гель, М.В. Салтевський, Г.С. Семаков. – К. : МАУП, 2001. – 216 с. – Бібліогр. : с. 211-212.
4. Усов А.И. Методы и средства решения задач компьютерно-технической экспертизы : учебное пособие. – М. : ГУ ЭКЦ МВД России, 2002. – 200 с.
5. Комп'ютерно-технічна експертиза (загальна частина): Методика / ДНДЕКЦ МВС України; Уклад. К.М. Ковальов, С.М. Корнійко, В.О. Княждвірський. – К., 2007.

ВИДИ І ЗАВДАННЯ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ

Юсіфлі Б. Т., студент 3-го курсу навчально-наукового інституту права та психології Національної академії внутрішніх справ

Комп'ютерно-технічна експертиза – самостійний рід судових експертиз, що відноситься до класу інженерно-технічних експертиз. КТЕ проводиться з метою: визначення статусу об'єкта як комп'ютерного засобу, виявлення та вивчення його ролі в розслідуваного злочині, а також отримання доступу до інформації на носіях даних з наступним всебічним її дослідженням.

Предмет КТЕ – факти та обставини, що встановлюються на основі спеціальних знань про технології розробки та експлуатації комп'ютерних засобів для реалізації інформаційних процесів.. Відповідно виділяються: апаратно-комп'ютерна експертиза; програмно-комп'ютерна експертиза; інформаційно-комп'ютерна експертиза. Крім того, досить виправданим видається введення ще одного виду КТЕ – комп'ютерно-мережевої експертизи. Такий поділ на види КТЕ найбільш повно охоплює технологічні