подлинность пользователя при его подключении к сети, но и подлинность пакетов, передаваемых между сервером и рабочей станцией.

Большую опасность представляют соединения пользователей по Интернет. Разнообразие методов доступа удаленных пользователей приводит к уязвимости информации и требует разнообразных методов защиты – таких как защита от фальшивых адресов, защита от перехвата, защита брандмауэром.

Литература: 1. Тихомиров В. П., Солдаткин В. И., Лобачев С. Л., Ковальчук О. Г. Дистанционное обучение: к виртуальным средам знаний (часть 1). – Дистанционное образование. – 1999. № 2. – С 8-15. 2. Андреев А. А., Солдаткин В. И. Дистанционное обучение: сущность. технология. – М: издательство МЭСИ. – 1999. – 196 с. 3. Бабушкин М., Иваненко С., Коростелев В. Веб-сервер в действии – СПб: Питер. – 1997. – 416 с. 4. Gasanov A. S., Melnyk I. V. Problems of defence and security of information in distance learning systems / Telematics and Life-Long Learning. Proceedings of the International Workshop. TLLL-2001. October 15-17, 2001, Kyiv, Ukraine. – P. 57. 5. Кухаренко В. М., Кудрявцева С. П., Колос В. В., Монако А. Ф., Цыбенко Ю. В. Основы Интернет. Дистанционный курс. – Харьков: ХДПУ – 1998. – 88 с. 6. Вакка Дж. Секреты безопасности в Internet. – К.: Диалектика. – 1997. – 512 с.

УДК 621.396

ДОСВІД ПІДГОТОВКИ ФАХІВЦІВ З ПИТАНЬ РОЗСЛІДУВАННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Володимир Голубєв

Центр Дослідження Проблем Комп'ютерної Злочинності

Анотація: **Розглянуто досвід впровадження дисципліни "Методика розслідування комп'ютерних злочинів" та підготовки фахівців-правоохоронців з питань попередження та розслідування комп'ютерних злочинів у Гуманітарному університеті "Запорізький інститут державного та муніципального управління".**

Summary: **Experience of introduction of discipline " The procedure of investigation of computer crimes " and preparations law enforcement on questions of the prevention and investigation of computer crimes at Humanitarian University " Zaporozhye Institute of the State and Municipal Management ".**

Ключові слова: **Навчання, методика розслідування, комп'ютерні злочини.**

I Вступ

Подібно багатьом революційним технологіям – комп'ютерні технології несуть з собою величезний потенціал як для прогресу так і для зловживань. Атаки у мережі, шахрайство, програмне піратство, технічне шпигунство, торгівля дитячою порнографією – тільки деякі зі злочинів, що вчиняються сьогодні у глобальній інформаційній мережі Internet.

Зростання науково-технічної озброєності злочинних угруповань об'єктивно впливає на використання правоохоронними органами сучасних інформаційних технологій, а також нових негласних засобів оперативно-розшукової діяльності (ОРД) у боротьбі зі злочинністю. Наприклад, жорсткі диски персональних комп'ютерів торговців наркотиками та зброєю можуть містити фінансові записи та дані щодо поставок та клієнтів. У випадку використання інформаційних технологій для планування або вчинення злочину з комп'ютера злочинця можна вилучити план вчинення пограбування або вбивства.

Для законного зняття комп'ютерної інформації потрібні спеціальні технічні засоби, у тому числі чітка юридична основа для установки таких засобів, але все це неможливо без спеціальної підготовки органів дізнання, суб'єктів ОРД.

Особливі труднощі викликають первісні слідчі дії, зв'язані з розслідуванням транснаціональних комп'ютерних злочинів (кіберзлочинів), що пов'язано з багатьма проблемами [1].

Результати досліджень, що проводяться Центром Дослідження Проблем Комп'ютерної Злочинності, та аналіз практичної діяльності правоохоронних органів щодо розслідування комп'ютерних злочинів свідчать, що дослідження комп'ютерної техніки, яка вилучається на місці події, доцільно проводити в умовах криміналістичної лабораторії, де цю роботу виконують фахівці з необхідною професійною підготовкою.

Інше питання, де сьогодні взяти таких фахівців, коли не один з ВУЗів України їх ще не готує. Отже, сьогодні назріла гостра потреба у підготовці та перепідготовці співробітників правоохоронних органів, які спеціалізуються у боротьбі з комп'ютерною злочинністю.

Як відомо перші кроки вже зроблені Донецьким юридичним інститутом МВС України. А з 1 вересня 2001 року у Гуманітарному університеті "Запорізький інститут державного та муніципального управління" розпочалось викладання дисципліни "Методика розслідування комп'ютерних злочинів".

II Основна частина

Програма курсу передбачає 8 тем, загальним обсягом 81 година, з яких 16 – лекційних годин, 18 годин – практичні заняття та 47 годин відведено на самостійну підготовку. Метою дисципліни «Методика розслідування комп'ютерних злочинів» є ознайомлення студентів з: поняттям і сутністю комп'ютерної інформації, основними засобами її зберігання та захисту, кримінально-правовою характеристикою комп'ютерних злочинів, криміналістичною характеристикою комп'ютерних злочинів, особливостями первісного етапу розслідування комп'ютерних злочинів, розслідування комп'ютерних злочинів на наступному етапі, попередження комп'ютерних злочинів, методикою попередження і розслідування транснаціональних злочинів, що вчиняються у сфері використання комп'ютерних технологій.

За стандартами Тема № 1 – Предмет та основні поняття дисципліни. У цій темі розглядаються: предмет та основні поняття дисципліни; поняття конфіденційності, цілісності та доступності інформації; причини зростання комп'ютерної злочинності; значення інформаційної безпеки в житті суспільства; правозастосовча практика діяльності правоохоронних органів з розкриття і розслідування злочинів у сфері комп'ютерної інформації; визначення основ державної політики в сфері захисту інформації в автоматизованих системах.

У наступній Темі № 2, яка називається "Поняття і сутність комп'ютерної інформації, основні засоби її зберігання та захисту", розглядаються питання, пов'язані з сутністю комп'ютерної інформації, її відмінність від інших видів інформації, основні способи збереження комп'ютерної інформації, основні засоби передачі комп'ютерної інформації, основні засоби і методи захисту комп'ютерної інформації.

Тема № 3 присвячена Кримінально-правовій характеристиці комп'ютерних злочинів. Вона передбачає розгляд об'єкту і предмету комп'ютерних злочинів, об'єктивний бік комп'ютерних злочинів, суб'єктивний бік комп'ютерних злочинів і його суб'єкту, обставини, що обтяжують відповідальність за вчинення комп'ютерних злочинів, відмінність комп'ютерних злочинів від суміжних складів злочинів.

У Темі № 4 "Криміналістична характеристика комп'ютерних злочинів" розглядаються дані про способи вчинення комп'ютерного злочину і механізму протиправних діянь, дані про способи приховування комп'ютерних злочинів, дані про знаряддя (засоби) комп'ютерних злочинів, дані про обстановку і місце здійснення комп'ютерних злочинів, дані про сліди комп'ютерних злочинів, дані про предмет злочинного зазіхання, дані про особу, що здійснює комп'ютерні злочини.

П'ята тема присвячена особливостям первісного етапу розслідування комп'ютерних злочинів. Це на мій погляд центральна тема курсу, тому що сьогодні саме на цьому етапі виникає найбільше помилок з боку правоохоронних органів. У цій темі розглянуті перевірочні ситуації, порядок одержання пояснень та огляд місця події. Розглянуті типові помилки, що виникають на цьому етапі при проведенні слідчих дій, пов'язаних з розслідуванням комп'ютерних злочинів. Нами особливо виділяються та вивчаються три типових помилки.

Помилка 1 – **Помилкова робота з комп'ютером.**

Перше та основне правило, що неухильно має виконуватися, полягає в наступному: ніколи і ні при яких умовах не працювати на вилученому комп'ютері. Це правило припускає, що вилучений комп'ютер – насамперед об'єкт дослідження фахівців. Тому його бажано навіть не включати до передачі експертам, оскільки категорично заборонено виконувати будь-які програми на вилученому комп'ютері без вживання необхідних заходів безпеки (наприклад, захисту від модифікації або створення резервної копії). Якщо на комп'ютері встановлена система захисту на вході в нього (наприклад – пароль), то його включення може викликати знищення інформації, що знаходиться на жорсткому диску. Не допускається завантаження такого комп'ютера з використанням його власної операційної системи.

Така міра пояснюється досить просто: злочинцю не складає особливих труднощів установити на своєму комп'ютері програму для знищення інформації на жорсткому чи гнучкому магнітному диску, записавши такі "пастки" через модифікацію операційної системи. Наприклад, проста команда DIR, яка використовується для відображення каталогу диска, може легко бути змінена, щоб відформовувати жорсткий диск.

Після того як дані і сама руйнуюча програма знищені, ніхто не зможе вірогідно сказати, чи був "підозрюваний" комп'ютер спеціально оснащений такими програмами, чи це результат недбалості при дослідженні комп'ютерних доказів?

Помилка 2 – **Допуск до комп'ютера власника (користувача) комп'ютера.**

Серйозною помилкою є допуск до досліджуваного комп'ютера власника для допомоги при його експлуатації. У багатьох зарубіжних літературних джерелах описуються випадки, коли підозрюваному на допиті, пов'язаному з комп'ютерними доказами, було надано доступ до вилученого комп'ютера. Пізніше вони розповідали своїм знайомим, як шифрували файли "прямо під носом у поліцейських", а ті при цьому

навіть не здогадувалися. Враховуючи таки наслідки, дуже швидко комп'ютерні фахівці стали робити резервні копії комп'ютерної інформації перш, ніж надавати доступ до них.

Помилка 3 – **Відсутність перевірки комп'ютера на наявність вірусів і програмних закладок.**

Для перевірки комп'ютера на наявність вірусів і програмних закладок необхідно завантаження комп'ютера не з операційної системи, що знаходиться у ньому, а з своєї, заздалегідь підготовленої дискети, або з стендового жорсткого диску. Перевірці підлягають усі носії інформації – дискети, жорсткий диск та інші носії. Цю роботу варто робити залученому для участі в слідчих діях фахівцю за допомогою спеціального програмного забезпечення.

Не можна допустити, щоб у суді з'явилася можливість обвинуватити слідство у навмисному зараженні комп'ютера вірусами, чи у некомпетентності при проведенні слідчих дій, або просто в недбалості, оскільки довести, що вірус був у комп'ютері до початку дослідження, навряд чи можливо, а подібне обвинувачення поставить під сумніви всю працю експерта та вірогідність його висновків.

Як свідчить практика – це найбільш типові помилки, що часто зустрічаються при дослідженні комп'ютера у справах, пов'язаних з розслідуванням комп'ютерних злочинів. Безумовно розглянутий перелік не охоплює всіх помилок, що виникають у процесі вилучення і дослідження комп'ютерної інформації.

Для запобігання помилкам при проведенні слідчих дій на початковому етапі розслідування, які можуть привести до втрати чи руйнування комп'ютерної інформації, вивчаються необхідні заходи і засоби запобігання помилковим діям.

У шостій темі "Розслідування комп'ютерних злочинів на наступному етапі", розглядається методика допиту обвинувачуваного та свідків, проведення очної ставки, призначення експертиз.

У темі 7 – "Попередження комп'ютерних злочинів", вивчаються обставини, що сприяють комп'ютерним злочинам, заходи та засоби попередження комп'ютерних злочинів.

Остання, 8 тема присвячена питанням попередження і розслідування транснаціональних злочинів, що вчиняються у сфері використання комп'ютерних технологій. І як завжди юридичні питання щільно зв'язані з технічними, а саме використанням міжмережних екранів для захисту комп'ютерних систем, положення Стразбургської конвенції щодо боротьби з кіберзлочинами [2], міжнародно-правові аспекти розслідування транснаціональних комп'ютерних злочинів. Більш детальніше з робочою та навчальною програмами курсу "Методика розслідування комп'ютерних злочинів" можна ознайомитися на нашому Web-сайті за адресою http://www.crime-research.org/library/Rabprog.htm [3].

Безумовно, як і всі інші види протиправних дій, транснаціональні комп'ютерні злочини (кіберзлочини) несуть у собі велику загрозу для людей, причому ступінь цієї загрози, на наш погляд, ще не до кінця усвідомлена й оцінена у нашому суспільстві. Але навіть той незначний досвід, що вже є в цій області, а тим більше досвід найбільш розвинутих країн світу, із всією очевидністю свідчить про безсумнівну уразливість будь-якої держави. Тим більше що транснаціональні комп'ютерні злочини не мають державних кордонів, і злочинець в однаковій мірі здатний загрожувати інформаційним системам, розташованим практично в будь-якій країні земної кулі. Такі злочини, як правило, виходять за рамки звичайних і нерідко являють собою нерозв'язні для діючого законодавства задачі. Особливий клопіт викликає проблема розслідування такого роду злочинів, сліди яких комп'ютерними злочинцями стираються та знищуються. При цьому розслідування таких злочинів може займати тижні, якщо не місяці, даючи можливість злочинцю знищити сліди злочину та уникнути покарання.

Декілька зауважень щодо наповненості практичних занять. Нами передбачено 4 практичних заняття, які проводяться у комп'ютерному класі. Тема першого заняття – "Захист файлів MS WORD з використанням параметрів доступу". Суть цієї роботи полягає в ознайомленні студентів та навчанні їх використанню стандартних методів Microsoft Word як парольного захисту файлів, так і за допомогою утиліти Msofpass.exe визначити пароль і відкриті файл для читання та правки.

Наступне практичне заняття № 2 присвячено парольному захисту архівних файлів та відповідно зворотних дій з визначення пароля та разархивування файлу.

На практичному занятті № 3 на базі використання відомої програми Folder Guard 4.08f, вивчається використання сучасних програмних засобів для розмежування прав доступу до логічних дисків, файлів і каталогів ПЕОМ.

І останнє, 4 практичне заняття передбачає роботу студентів у мережі Inetrnet, та полягає у практичному використанні методів комп`ютерної стеганографії. З методичними вказівками з проведення практичних занять з дисципліни "Методика розслідування комп'ютерних злочинів" можна ознайомитися на нашому Web-сайті за адресою http://www.crime-research.org/library.html .

III Висновки

На наш погляд, при підготовці дисципліни “Методика розслідування комп’ютерних злочинів” були враховані вади та недоліки професійної підготовки працівників правоохоронних органів, що спеціалізуються з питань попередження і розслідування комп'ютерних злочинів.

Тенденція росту комп’ютерної злочинності та тенденція "відставання" соціально-правового контролю над нею перетворюється в деяке хибне коло, розірвати яке можна тільки шляхом органічного сполучення кримінально-правової і криміналістичної стратегії боротьби з цим видом злочинів. Причому важливою складовою такої стратегії має стати підготовка та перепідготовка фахівців правоохоронців в умовах впровадження і використання сучасних комп’ютерних технологій.

Підсумовуючи викладене, треба зазначити, що питання підготовки фахівців з питань розслідування комп’ютерних злочинів слід вирішувати терміново і в інших профільних (юридичних) ВУЗах України. Першим кроком, який можна зробити вже сьогодні, є організація відповідних спеціалізацій при існуючих спеціальностях. Найважливішою задачею також є підготовка умов створення нових спеціальностей з підготовки таких фахівців, перш за все приділивши увагу формуванню викладацького складу та спеціалістів, що зможуть підготувати методичне забезпечення, підручники тощо.

Література: 1. Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп’ютерних технологій. – Запоріжжя: Просвіта, 2001.– С. 198-201. 2. Draft Convention on Cyber-crime. STRASBOURG, 27.04.2000 – COUNCIL OF EUROPE. http://www.crime-research.org/library/Draft27.html. 3. Програма курсу “Методика розслідування комп’ютерних злочинів”, http://www.crime-research.org/library/Rabprog.htm.