У рамках першого підходу всі дослідження проводяться з образом носія засобами програмного забезпечення, за допомогою якого він був створений або дозволяє переглядати його та дослідити (WinHex/X-Ways Forensics, Encase, ILook тощо). Якщо ці засоби не забезпечують всебічне дослідження, можна скопіювати необхідну інформацію на носій експерта (назвемо його експериментальним) і продовжити подальші дослідження на експериментальному носії спеціалізованими програмними засобами для цього виду інформації.

У разі завантаження ОС із зовнішнього носія та дослідження НЖМД безпосередньо у складі наданого ПК (тобто «наживо») інформація досліджується програмними засобами, які містяться на зовнішньому носії. Необхідно, аби до їхнього складу входили як мінімум файл-менеджер, спеціалі-зовані програмні засоби для певного виду інформації й програми з відновлення видаленої та ушкодженої інформації.

Якщо запровадити третій (нетрадиційний) підхід, то інформація може досліджуватися як засобами, що містяться на НЖМД, так і, якщо їх недостатньо, додатково спеціалізованими програмами, котрі можна завантажувати із зовнішніх носіїв.

У необхідних випадках можна комбінувати застосування підходів, наприклад, перший і третій.

Уважаємо за доцільне продовжити дослідження в цьому напрямі у зв'язку з подальшим розширенням застосування всесвітньої мережі Інтернет, розробленням та появою нових Інтернет-браузерів (наприклад Google Chrome) і нових операційних систем.

КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Добришин Ю.Є., кандидат технічних наук, доцент, заступник директора Коледжу економіки, права та інформаційних технологій Університету «КРОК»

Семенов В.В., кандидат юридичних наук, доцент, доцент кафедри кримінально-правових ННІПП НАВС

У зв'язку з відносною новизною комп'ютерної злочинності не можна не виділити серед основних напрямів організації їй протидії необхідність створення ефективної системи професійної підготовки кадрів.

Одним із основних завдань даного напряму, є створення у відомчих установах сучасної кадрової, методичної і матеріально-технічної бази підготовки і перепідготовки потрібних фахівців. Система підготовки кадрів повинна підкріплюватися науковими дослідженнями відповідного профілю.

Розвиток подібної системи повинен не тільки виходити з вимог сьогодення, але і враховувати тенденції зміни злочинності в майбутньому. Формування кадрового ядра спеціалізованих підрозділів правоохоронних органів повинне включати три важливі напрями: професійну підготовку, перепідготовку і підвищення кваліфікації їх співробітників. При цьому особливу увагу слід приділяти останньому напряму: кожен працівник, який залучений до діяльності в даному напрямі, повинен регулярно проходити навчання, з тим щоб бути в курсі новацій у сфері технологій і юридичної практики, що склалася.

Комплекс необхідних професійних якостей осіб, задіяних по лінії боротьби із комп'ютерною злочинністю, крім звичайних (надійність, компетентність і професіоналізм, добре розвинена пам'ять, схильність до аналізу, пунктуальність і т. д.), повинен включати деякі додаткові вимоги. Наприклад, такі як:

– навички спілкування в «комп'ютерних» колах, розуміння особливостей цього середовища, володіння лексикою що використовується в ньому;

– знання сучасних операційних систем;

– розуміння механізмів злому комп'ютерних систем і відповідних методів протидії;

– уміння читати і аналізувати складні системні файли (журнали реєстрації подій, файли настройки конфігурації і т. п.),

виконувати аналітичний пошук кореляції між подіями або сигнатурами нападу, визначати тип загрози;

– володіння апаратними і програмними засобами фіксації отриманої інформації і виявлення підозрілих подій;

– уміння доступно висловлювати в документах і усно складну технічну інформацію.

Для розуміння явищ, що відбуваються в інформаційному середовищі, все частіше потрібні глибокі знання самих різних аспектів функціонування сучасного суспільства. До аналітичної роботи необхідно залучати фахівців з різносторонньою підготовкою. Вони повинні бути здатні враховувати різноманітні чинники мотивації комп'ютерних злочинів, бути досвідчені в різних сферах (технічної, економічної, соціальної, юридичної і ін.).

Недостатній рівень теоретичної і практичної підготовки співробітників правоохоронних органів в даній сфері пов'язаній і із слабкою забезпеченістю науковими дослідженнями відповідного профілю. В зв'язку з цим представляється перспективною організація спеціалізованих структур із проблем комп'ютерної злочинності, завданням яких е вивчення, розробка стратегічних і тактичних підходів до розкриття комп'ютерних злочинів на основі комплексного вивчення тенденцій комп'ютерних кримінальних процесів. Безперечну користь могло б принести створення центру аналізу комп'ютерних злочинів, покликаного здійснювати аналітичну і методичну діяльність, інформування громадськості про загрози, які несе комп'ютерна злочинність, а також розроблення методів профілактики.

Не менш складну проблему становить недостатня забезпеченість спеціалізованих підрозділів засобами обчислювальної техніки, спеціальними приладами і устаткуванням. Тим часом від такої оснащеності залежить не тільки результативність розслідувань, що провадяться, але і, що не менш важливо, якість криміналістичних експертиз, пов'язаних з аналізом доказів в електронному вигляді. Подібні експертизи

нерідко пов'язані з необхідністю аналізу справді гігантських об'ємів комп'ютерних даних.

Ефективність науково-дослідних робіт, направлених на попередження та розслідування комп'ютерних злочинів, також багато в чому визначається рівнем забезпеченості технічними засобами та програмними продуктами. І безумовно, технічне оснащення безпосередньо визначається фінансовими вкладеннями в цю сферу.

Підводячи підсумок викладеному, необхідно ще раз підкреслити, що підвищення ефективності боротьби із комп'ютерною злочинністю безпосередньо пов'язано з комплексним рішенням означених проблем. І можна констатувати, що передумови для цього є, оскільки теорією в основному вироблені, а практикою постійно удосконалюються відповідні рекомендації в даній сфері.

АКТУАЛЬНІ ПИТАННЯ ТА ПРАВОВІ ПІДСТАВИ ПРИЗНАЧЕННЯ СУДОВОЇ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ

Кубрак Т. І. студент Київського національного університету культури і мистецтв

Залучення експерта для проведення судових експертиз під час кримінального провадження, оформлення їх результатів, права сторін, а також права, обов'язки та відповідальність судового експерта регулюється Кримінальним процесуальним кодексом України (далі – КПК) (статті 36, 39, 40, 42, 44, 46, 47, 56–59, 69–70, 242–245, 332 КПК та ін.) [1]. Порядок проведення судових експертиз також детально врегульований Інструкцією про призначення та проведення судових експертиз та експертних досліджень, (далі – Інструкція) [2].

Дослідженню судової комп'ютерно-технічної експертизи (далі – СКТЕ) присвятили свої наукові праці В.Б. Вєхов, І.В.