При проведенні зазначених вище експертиз об'єктом дослідження, як правило виступають:

– комп'ютерно-технічні засоби (системні блоки персональних комп'ютерів та серверів, ноутбуки, нетбуки, планшети тощо);

– носії комп'ютерної інформації (накопичувачі на жорстких та гнучких магнітних дисках, лазерні оптичні диски та приводи до них, флешносії тощо);

– периферійна техніка (сканери, принтери, багатофункціональні пристрої тощо);

– телекомунікаційне мережеве обладнання (комутатори, маршрутизатори, модеми тощо);

– термінали рухомого мобільного зв'язку (мобільні телефони, 3G-модеми) тощо.

Для проведення криміналістичного дослідження зазначених об'єктів експерт повинен використовувати затверджені методики [4] та використовувати спеціальне криміналістичне обладнання та програмне забезпечення.

При цьому, криміналістичне обладнання та програмне забезпечення, що використовується для проведення експертиз, у зв'язку з тим, що об'єктами дослідження можуть бути пристрої різних типів підключення та фірм розробників (наприклад, накопичувачі на жорстких дисках типом інтерфейсу підключення IDE, SATA або SCSI; мобільні телефони на базі операційної системи Android або iOS; тощо) повинно бути багатофункціональним та мати, за можливості, програмні інструменти необхідні для проведення повного та якісного дослідження (наприклад, функцію копіювання вмісту носія інформації, відновлення видаленої інформації, контекстний пошук тощо).

Таке криміналістичне обладнання та програмні продукти можна поділи на такі основні групи:

– блокувачі запису, що гарантують випадкове невнесення змін до носія інформації, якій досліджується під час проведення експертного дослідження;

– засоби для зйому інформації з накопичувачів на жорстких магнітних дисках;

– засоби для зйому інформації з терміналів мобільного зв'язку.

На теперішній час експерти мають можливість вибирати із запропонованих фірмами-розробниками різні програмні продукти та криміналістичне обладнання. Всі вони відрізняються своїми базовими функціональними можливостями, а відповідно і ціною. Тому обрання певного програмного чи апаратного продукту є не тривіальною задачею та потребує проведення порівняння технічних характеристик цих продуктів й обрання одного з них за певними критеріями.

Список використаних джерел:

1. Кримінальний Кодекс України : закон України від 05.04.2001 № 2341-III [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2341-14. – Редакція від 23.10.2014.

2. Кримінальний процесуальний Кодекс України : закон України від 13.04.2012 № 4651-VI [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/4651-17. – Редакція від 22.08.2014.

3. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ М-ва юстиції України від 08.10.1998 № 53/5 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/z0705-98. – Редакція від 22.01.2013.

4. Реєстр методик проведення судових експертиз / М-во юстиції України [Електронний ресурс]. – Режим доступу: http://rmpse.minjust.gov.ua.

Одержано 29.10.2014

УДК 004.738

Віталій Анатолійович СВІТЛИЧНИЙ,
викладач кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ;

Костянтин Едуардович ПЕТРОВ,
доктор технічних наук, професор,
професор кафедри інформаційних технологій та захисту інформації
факультету права та масових комунікацій
Харківського національного університету внутрішніх справ

ВІД ІДЕНТИФІКАЦІЇ КОМП'ЮТЕРА ДО ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА У МЕРЕЖІ ІНТЕРНЕТ

Однією з проблем з якою стикається працівник правоохоронних органів при розслідувані злочинів, які були здійсненні через мережу Internet є визначення комп'ютера користувача мережі з якого були здійснені кримінальні дії (кіберзлочини). Погрішність ідентифікації, заснованої на IP-адресі (до недавнього часу облік був основним методом ідентифікації), складається з погрішностей передачі і погрішностей користування комп'ютером. Так, наприклад, при роботі користувачів через proxy-сервер уся підмережа, яка за ним ховається, у більшості випадків матиме єдиний IP-адрес. З іншого боку, працюючи через комутоване з'єднання, користувач при кожному підключенні отримуватиме від провайдера новий IP-адрес і т. д.

Завдання ідентифікації користувача не втрачає своєї актуальності в зв'язку постійною гонкою технологій захисту інформації і технологій неправомірного отримання доступу до інформації. Актуальність цього завдання для мережі Інтернет підвищується використанням незахищених каналів передачі даних.

Завдання ідентифікації пристрою зазвичай вирішується за допомогою унікальних кодів таких як MAC або IP-адрес в мережах Ethernet або IMEI в мережах GSM. Проте використання унікального коду дає відповідь на питання те ж цей пристрій або ні, але не повідомляє точний тип пристрою і спосіб його використання конкретним користувачем. Окрім ідентифікаторів, можливе використання додаткової інформації, яка затребувана у разі обробки непрямих ознак, на підставі інформації отримуваної з датчиків пристрою і в результаті роботи програмного забезпечення на пристрої. В даному випадку мається на увазі визначення типу діяльності користувача за даними глобальних систем позиціонування і гіроскопа, а також застосування методів динамічної і статичної біометрії, таких як, рисунок вен на долоні, відбиток пальця, веселкова оболонка ока, геометрія кисті руки або особи, 3D-проекція черепа, клавіатурній почерк, форма вуха, голос і будь-яка інша відмітна ознака може служити для ідентифікації людини біометричною системою.

Використовуємо поняття відбиток пристрою, стосовно інформації що залишається на серверах і інших пристроїв реєстрації, а поняття відбиток особи в пристрої до інформації що побічно характеризує людину за інформацією що залишилася у використаному їм пристрої. Прикладом відбитку пристрою служить запис в log-файлі сервера, а відбитком особи інформація про використані програми, час і тривалість використання програм, набір використаних файлів і інших ресурсів.

Особливе місце серед програмного забезпечення з точки зору завдання ідентифікації пристрою займає браузер, як програма, за допомогою якої користувач дістає доступ до більшості Internet-ресурсів. Для ідентифікації використовується інформація cookies-файлів та інформація про встановлені шрифти і плагінах. Вирішуючи задачу ідентифікації з використанням непрямих ознак, слід враховувати швидкість зміни конфігурацій апаратного і версій програмного забезпечення вживаного користувачем, а так само біологічні ритми до яких схильна людина. Динамічні біометричні ознаки людини змінюються впродовж півроку. Статичні біометричні ознаки зберігаються упродовж усього життя.

Рішення задачі ідентифікації людини і пристрою використовуватиметься при реалізації концепції «програмний агент», для визначення психофізіологічного стану людини і в завданнях з області безпеки, для створення механізмів відстежування шляху. Ідентифікація пристрою і людини є проміжними цілями. Завдяки ідентифікації пристрою можливе калібрування методів знімання інформації. Кінцевою метою ідентифікації пристрою є ідентифікація людини, отримання прямої або непрямої інформації про нього.

Початковими даними для ідентифікації пристрою і людини пропонується вважати: інформацію про пристрій, інформацію про навколишній світ, інформацію про людину. Складність формалізації початкових даних полягає в неможливості побудови вичерпної безлічі значень деяких ознак. Інформація про використання клавіатури складається з коду клавіші, часу події, типу події. Проте формалізувати ознаку, пов'язану з граматичними і орфографічними помилками що допускаються користувачем при наборі тексту, як мінімум, складно.
Інформація про пристрій складається з: списку і конфігурації використовуваного апаратного забезпечення; списку і конфігурації встановлених програм, і, якщо це можливо, часу установки програм; інформації збереженої на облаштуванні користувача у вигляді cookies-файлів, інших тимчасових файлів; відбитку файлової системи пристрою.

Під відбитком файлової системи розуміється інформація про структуру файлової системи, а не отримання математичної свертки даних у файловій системі. Особлива увага приділяється файлам старше за місяць, в яких не відбувалося змін за цей час. Вони мають достатню стабільність, щоб на деякий час стати ідентифікуючою ознакою. Для створення відбитку файлової системи пропонується використовувати інформацію про їх ім'я, місце розташування, розмір, дату створення і дату редагування.

Інформація про користувача складається з: днів тижня, часу доби використання, тривалості активності програмного забезпечення; друкарських помилках, що повторюються, словах паразитах, помилках при наборі тексту; подіях миші або клавіатури.

Кінцевою метою дослідження завдання ідентифікації людини і пристрою є побудова розпізнавача, здатного із задовільною точністю робити ідентифікацію. Особливість цього пристрою полягає в непостійному наборі вхідних значень, що повинне відбиватися на його внутрішній структурі.

Одержано 09.10.2014