МЕТОДИКА ПРОВЕДЕННЯ ЦИФРОВОЇ ЕКСПЕРТИЗИ ЕНЕРГОЗАЛЕЖНОЇ ПАМ'ЯТІ КОМП'ЮТЕРІВ В ІНТЕРЕСАХ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

канд.техн. наук, доц. А.В. Снігуров, магістр М.С. Сірий, Харківський національний університет радіоелектроніки, м. Харків

Цифрова криміналістика на сучасному етапі це відносно новий вид криміналістики, при якому проводиться дослідження цифрових пристроїв для знаходження цифрових слідів злочинів. Існує багато методів отримання цифрових доказів, одним з яких є так звана "Жива (Live)" криміналістика. Даний вид цифрової криміналістики використовується для пошуку цифрових доказів в працюючій системній середі. Тобто при вилученні цифрових пристроїв на місті проведення слідчих дій, якщо комп'ютерна техніка не вимкнена і до неї є доступ, є можливість отримати значну кількість інформації з цієї техніки. Відповідно до цього актуальним завданням є створення методик та технік проведення цифрових досліджень, в тому числі і для цифрової експертизи енергозалежної пам'яті комп'ютерної техніки.

В доповіді приводяться результати аналізу особливостей зміни даних комп'ютерів під час процесу їх отримання експертом та залежність проведення експертизи від типу операційної системи. Приводиться аналіз антикриміналістичних (anti-forensic) технік і засобів.

Також в доповіді приведена методика проведення експертизи працюючого комп'ютера з використанням команд операційної системи Windows, інструментів Sysinternals Tools [1], утиліт Nirsoft [2] та інших інструментів. В доповіді приведені дані по інформації, що отримується, та приклади на реальному комп'ютері: системна інформація та налаштування, інформація о процесах і службах, що запущені, інформація про мережеві підключення, кеш ARP, інформація про відкриті дескриптори для кожного з процесів, інформація про усіх користувачів, що увійшли у систему, незбережені документи та інше. Результати, що приведені в доповіді, планується також використовувати для розробки методик виявлення та аналізу сучасних кібератак на об'єкти критичної інфраструктури.

Список літератури: 1. Microsoft Ignite. Sysinternals. [Електронний ресурс]. Режим доступу до ресурсу: https://docs.microsoft.com/en-us/sysinternals/. **2.** Nirsoft. [Електронний ресурс]. Режим доступу до ресурсу: https://www.nirsoft.net/.