УДК 004.076.4

Автоматизация процесса проведения расследования преступлений, совершенных с использованием средств вычислительной техники.

Автор: Кочуров Е.А., Университет ИТМО, Санкт-Петербург

Научный руководитель: Комаров И.И., Университет ИТМО, Санкт-Петербург

Постановка проблемы. Повсеместный процесс информатизации общества влечет за собой интеграцию информационных технологий во все сферы деятельности человека, в том числе и в процесс осуществления противоправных действий различного характера. Скорость развития информационных технологий и их разнообразие порождают следующие факторы, совокупное влияние которых негативно сказывается на качестве и скорости расследования преступлений, совершенных с использованием средств вычислительной техники:

1. Необходимость обладания специальными техническими познаниями в области информационных технологий сотрудниками, осуществляющими процесс расследования преступлений, совершенных с использованием средств вычислительной техники;
2. Быстрое устаревание существующих методик исследования средств вычислительной техники;
3. Необходимость обработки большого объема данных при сборе доказательной базы;
4. Нарушение целостности информации, хранящейся на накопителях, вследствие неправильного обращения со средством вычислительной техники при проведении исследования на месте.

Цель работы. Формализация этапов проведения постинцидентного исследования средств вычислительной техники; разработка комплекса методов анализа и классификации информации, содержащейся в энергонезависимой памяти средств вычислительной техники; автоматизация разработанных методов с целью повышения качества и скорости выполнения ряда этапов проводимого исследования; разработка механизма автоматизированного формирования базы знаний по проводимым исследованиям для последующего их использования с целью повышения эффективности использования обнаруженной информации.

Промежуточные результаты. Построена обобщенная модель поиска и классификации информации, содержащейся в энергонезависимой памяти средств вычислительной техники, и определения ее релевантности и информативности в разрезе проводимого исследования; формализованы этапы проведения постинцидентного анализа средств вычислительной техники; разработаны общие модели базы знаний, учитывающие специфику проведения исследований по основным направлениям.

Основной результат. Разработка комплекса программного обеспечения, собирающего воедино и реализующего на практике полученные в ходе исследования методики и механизмы, способного рационально решить вышеупомянутые проблемы и, тем самым, повысить общую эффективность проведения расследования преступлений, совершенных с использованием средств вычислительной техники.