УДК 004.076.4

РАЗРАБОТКА МЕТОДИКИ АВТОМАТИЗАЦИИ ПОСТИНЦИДЕНТНОГО АНАЛИЗА НА ОСНОВАНИИ КОМБИНАЦИЙ ОСТАТОЧНЫХ ПРИЗНАКОВ

Ширяев А.А. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)
Научный руководитель – к.т.н., Таранов С.В. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Аннотация.
В работе представлен подход к обеспечению ускоренного автоматизированного процесса проведение компьютерно-технических экспертиз с увеличением точности сбора доказательной базы. Представленный подход позволяет автоматически формировать предварительную оценку наличия следов компьютерного инцидента.

Введение.
В связи с постоянной информатизацией общества, а также модернизацией его бытовых и коммерческих процессов, мы сталкиваемся с ощутимым ростом количества инцидентов, так или иначе связанных с компьютерной техникой. Растущий объем и непрерывная изменчивость таких инцидентов сильно увеличивают требования к эксперту. Порядок проведения компьютерно-технических экспертиз вынуждает эксперта значительную часть времени тратить на поиск и сбор предположительно необходимых для ответов на поставленные ему вопросы данных, в то время как сроки, отведенные под установление обстоятельств произошедшего, как правило, ограничены. Между тем, в условиях увеличенной на эксперта нагрузки возрастает влияние человеческого фактора на результаты исследования.

Основная часть.
Разработана методика постинцидентного анализа информации, содержащейся в энергонезависимой памяти средств вычислительной техники. С целью повышения скорости поведения исследования и его качества методика включает в себя использование механизма автоматизации, нацеленного на предварительное обнаружение информации и ее классификацию с точки зрения релевантности в данном исследовании. Засчет предварительной систематизации и дальнейшего использования паттернов комбинаций остаточных признаков, подход позволяет применить математический алгоритм и решить ряд проблем – необходимость обработки большого объема данных для сбора доказательной базы, вероятность нарушения целостности информации при длительном анализе и необходимость обладание глубокими знаниями по каждому типу инцидента.

Выводы.
Описанная методика была опробована на практике и сравнена с классическим подходом без использования автоматизации. Моделирование показало прирост производительности в 2-3 раза. Дальнейшие исследования будут связаны с расширением сферы применения методики и уменьшением доли человеческого участия в процессе.

Ширяев А.А. (автор) _____

Таранов С.В. (научный руководитель) _____