ИНФОРМАЦИОННО-КОМПЬЮТЕРНАЯ ЭКСПЕРТИЗА (ДАННЫХ), НАПРАВЛЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Д.В. Липень, Д.В. Михейчик

Информационно-компьютерная экспертиза (данных) является ключевым видом судебной компьютерно-технической экспертизы, так как позволяет создать доказательственную базу путем решения диагностических и идентификационных задач, связанных с компьютерной информацией. Целью этого вида СКТЭ является поиск, обнаружение, восстановление, анализ и оценка информации на машинных носителях, подготовленной пользователем или порожденной (созданной) программами для организации информационных процессов в компьютерной системе. Исключительно на выводах подобной экспертизы стоится доказательная база при обвинении в совершении преступлений в области информационной безопасности.

Основными машинными носителями на сегодняшний день являются накопители на жестких магнитных дисках (винчестеры) или НЖМД. Поэтому в лаборатории судебных компьютерно-технических исследований НИИ КиСЭ Министерства юстиции Республики Беларусь ведется разработка методических рекомендаций по проведению криминалистического исследования НЖМД, разработка научно обоснованных подходов для криминалистического исследования имеющейся на них информации (в том числе и удаленной), разработка подходов к считыванию информации с технически неисправных НЖМД, разработка общей схемы проведения подобных исследований неповреждающими методами. Отдельное внимание уделяется формам представления информации и способам ее сокрытия.

Проведен анализ алгоритмов работы специализированных программ поиска информации "Encase Forensic Edition", "ILOOK Investigator", "Vogon International". Наиболее перспективным признан "Encase Forensic Edition", поскольку реализованная в нем хэш-функция "криминалистического образа" позволяет полностью исключить изменения данных недобросовестным следователем или экспертом. Более того, "Encase Forensic Edition" представляет собой "концепцию программной среды, адаптированной к продвинутому поиску информации" и позволяет "подключать" шаблоны и модули иных разработчиков ПО.