Т. А. Плотникова (Ставрополь СГУ)**. Информационные следы и методы их поиска.**

Востребованность средств защиты цифровой информации от несанкционированного доступа, в том числе с использованием криптографических средств защиты информации порождает обратную задачу — задачу поиска ценной информации среди зашифрованной в больших массивах данных.

В ходе исследований, была выявлена методика обнаружения использования средств криптографического преобразования. Для проведения данной методики необходимо выполнить ряд этапов.

Подготовительный этап настоящей методики включает исследование данных окружения — т. е. данных, имеющих непосредственное отношение к объекту исследования. Например, в наиболее распространенном случае — необходимо проанализировать операционную систему на предмет наличия сведений об установке (удалении) программных и программно-аппаратных средств криптографической защиты информации.

На первом этапе производится исследование реестра операционной системы. В реестре операционной системы создаются журналы, в которых отражается процесс криптографического преобразования (шифрования) информации.

На втором этапе необходимо проверить файловую систему. При рассмотрении файловой системы, из общего потока информации шифртекст выделяется наличием собственных, не похожих на другие, сигнатур в заголовке. Под сигнатурами будем понимать уникальную последовательность байтов, принадлежащую конкретному известному типу файлов и не встречающуюся в других типах [1]. Сигнатуры информации, подвергшейся криптографическому преобразованию, являются уникальными и, при сравнении со справочником сигнатур, не могут быть найдены в справочнике.

На заключительном этапе методики исследуется общее содержание файлов данных. Криптографическое преобразование данных приводит к «замене» имеющейся в файле информации псевдослучайной последовательностью. Наличие данного также свидетельствует о возможности зашифрования информации [2].

Таким образом, в результате применения настоящей методики становится возможен эффективный поиск следов зашифрованной информации, представленной в виде отдельных файлов или каталогов на носителях цифровой информации различного типа, с различными файловыми системами.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 5118898. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. М.: Госстандарт России, 1998.
2. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003