реализующих угрозы, и созданные на их основе программные комплексы как раз и помогают достичь такого компромисса.

В качестве примера применения на практике подобного рода моделирования в Республике Беларусь можно привести работу по анализу эффективности системы физической защиты ОИЯЭИ «Сосны», проведенную в октябре 2009 г. в Лепеле совместно с американскими специалистами из Министерства энергетики США и Окриджской национальной лаборатории по учету, контролю и физической защите ядерных материалов. В результате моделирования нарушителей и розыгрыша трех сценариев реализации угроз был сформулирован четкий план по наращиванию системы охраны объекта.

УДК 343.98

*В.Е. Козлов*

-

Материальная сущность компьютерной информации (КИ) позволяет выделить ее важнейшее свойство, проявляющееся в процессе отражения – свойство информационной вещи (объекта), предмета. Обработка, тиражирование, накопление, хранение КИ осуществляется в форме файла, под которым традиционно понимают поименованную совокупность записей, хранящихся или обрабатываемых как единое целое. Средством работы с файлами являются средства компьютерной техники (СКТ). В результате действий человека, совершаемых в отношении КИ с использованием СКТ, происходит создание, удаление файла, изменение его содержания (составляющих сведений о лицах, предметах, фактах, событиях, явлениях и процессах), атрибутов. Такие действия сопровождаются процессами следообразования. Распространяя системно-логический подход на деятельность, содержание которой состоит в собирании доказательств по делам о высокотехнологичных (компьютерных) преступлениях, можно сделать следующие выводы.

Компьютерные файлы, содержащие оперативно-розыскную информацию, как правило, не являются электронными документами в информационно-правовом смысле. Такое название им можно дать с определенной долей условности. В процессе выявления и раскрытия компьютерных преступлений такой термин может быть использован в более широком собирательном понимании.



Существует система признаков, позволяющих идентифицировать КИ в форме файла (файловой системы), которая включает:

свойства (параметры): признаки, атрибуты, содержание и т. д. файла как предмета материального мира; условия обстановки совершения компьютерного преступления, т. е. среду, в которой производились действия по приготовлению, совершению и сокрытию его, а также условия среды, в которой осуществлялось документирование файла при проведении оперативно-розыскного мероприятия (ОРМ). Отсутствие одного из названных элементов системы признаков не допускает последующей идентификации файла как документа.

Документирование при проведении ОРМ предполагает сохранение копий файлов, каждая из которых обеспечивает целостность КИ, полностью характеризует оригинал, и однозначно определяет его существование.

Для получения копии файла используются отчуждаемые носители субъекта, осуществляющего документирование. Таковыми могут быть магнитные, оптические, магнитооптические, полупроводниковые (как правило, энергонезависимые) и иные типы отчуждаемых носителей, появляющиеся по мере их разработки и внедрения в отрасли информатизации. При этом сам отчуждаемый носитель, не содержащий КИ, никакого последующего доказательственного значения не имеет (за исключением случаев, когда он содержит следы, отличные от образующихся в результате воздействия СКТ на компьютерную информацию, – следы пальцев рук, механических повреждений и т. д.), а приобретает его в момент окончания записи копии файла на него.

В процессе документирования по делам о компьютерных преступлениях определяющую роль играет нормативно закрепленная процедура действий с файлом, придающая его копии юридическую силу и позволяющая субъекту ОРД одновременно с фиксацией и изъятием файла (копированием на носитель) осуществлять документирование элементов среды его существования. Специальные требования к подобной процедуре (цели и задачи, условия, порядок и субъекты производства, допустимость применения тех либо иных методов и средств собирания доказательств, способы оформления результатов и т. д.) устанавливаются оперативно-розыскным законодательством.

Последовательность и результат выполнения таких действий должны документироваться по правилам, установленным оперативно-розыскным законодательством.