И.Г. Кудрин
ВА РБ (Минск)

О НЕКОТОРЫХ АСПЕКТАХ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечение инфорхмационной безопасности является одним из важнейших условий дальнейшего прогрессивного развития Республики Беларусь. Возросшие требования современности к защите интересов личности, общества, государства от внешних и внутренних угроз в информационной сфере реализованы в деятельности правоохранительных органов. К числу таких угроз Концепция национальной безопасности Республики Беларусь относит рост преступности с использованием информационно-коммуникационных технологий.

На современном этапе распространение получили мошенничество с электронными платежными средствами, хищения конфиденциальной информации, уничтожение электронных документов и иные подобные правонарушения.

Для решения задач расследования указанных и других преступлений против информационной безопасности в криминалистике продолжает развитие направление, получившее наименование «форензика». Термин «forensics» является сокращенной формой «forensicscience», дословно «судебная наука». При заимствовании в русский язык слово в определенной мере сузило свое значение и означает компьютерную криминалистику Данное направление появилась с момента первых преступлений совершенных при помощи компьютера.

Более тесные связи форензики прослеживаются с технико-криминалистическим исследованием документов, так как компьютеры и компьютерная периферия в настоящее время чаще других применяются при подделке документов различных видов.

В форензике выделяется самостоятельный раздел, связанный с исследованием программ для ЭВМ. В рамках указанного раздела решаются задачи по изучению устройства программ по исполняемому коду, методы создания вредоносных программ, противодействия им и иные, что требует специфических методов, существенно отличающихся от других методов форензики, применяемых для поиска, сбора и исследования цифровых доказательств.

В юридической литературе к предмету форензики отнесены: криминальная практика - способы, инструменты совершения соответствующих преступлений, их последствия, оставляемые следы, личность преступника; оперативная, следственная и судебная практика по компьютерным преступлениям; методы экспертного исследования компьютерной информации и, в частности, программ для ЭВМ; достижения отраслей связи и информационных технологий, их влияние на общество, а также возможности их использования как для совершения преступлений, так и для их предотвращения и раскрытия.

В рамках расследования обозначенных преступлений целесообразно учитывать специфику их следовой картины. В большинстве случаев следы,

с которыми приходится работать специалисту по форензике, представляют собой компьютерную информацию, регулярную или побочную. Их достаточно легко уничтожить - как умышленно, так и случайно. Часто их легко подделать, ибо «поддельный» байт ничем не отличается от «подлинного».

Фальсификация электронных (цифровых) данных выявляется по смысловому содержанию информации, либо по оставленным в иных местах следам, как правило, информационным. Цифровые сведения не воспринимаются органами чувств человека. Это возможно через достаточно сложные аппаратно-программные средства. Поэтому следы указанного вида сложно продемонстрировать участникам уголовного процесса. Определенную сложность на практике представляют вопросы обеспечения неизменности таких следов при их хранении и использовании. На отдельных видах носителей она хранится статически в виде разной намагниченности участков носителя или вариаций его оптических свойств. В других случаях метод хранения информации связан с постоянной сменой носителя.

Представляется, что отдельные положения форензики могут быть востребованы при дальнейшей разработке частной видовой криминалистической характеристики отдельных преступлений против информационной безопасности, определении особенностей тактики следственных действий, оперативно-розыскных мероприятий по данной категории преступлений, создании методов, аппаратных и программных инструментов для сбора и исследования доказательств, иным, связанным с указанными направлениям.

Частные видовые криминалистические характеристики предоставят возможность полуения и систематизации на практике новых криминалистически значимых сведений о рассматриваемых преступлениях, будут способствовать повышению качества решения задач расследования его субъектами. Установление связей зависимости между структурными элементами указанных характеристик позволят с высокой степенью вероятности определять поисковые признаки неизвестных элементов. Это способствует повышению результативности расследования при наименьших затратах сил, средств и времени.

Таким образом, основные положения форензики могут быть применены: в расследовании преступлений, где в качестве объекта посягательства выступают компьютерная информация, компьютер как орудие совершения и сокрытия преступления; при сборе и исследовании материалов, представленных в виде компьютерной информации (программа для ЭВМ, иное произведение в цифровой форме, товарный знак в сети Интернет, доменное имя и др.); в военной сфере при решении задач по оказанию воздействия на информационные системы противника и защите своих систем и др.

Реализация положений форензики в этой связи будет способствовать сведению до минимума ошибок организационного и тактического характера, конкретизации задач, упорядочению и оптимизации процесса расследования указанных преступлений, дальнейшему обеспечению прав граждан и государственных интересов.