блюдать условия заключенных с оперативно-розыскным органом контракта или договоренности о сотрудничестве; не допускать умышленного представления заведомо ложной информации; сохранять в тайне сведения, которые стали им известны при подготовке или проведении ОРМ.

Одним из элементов статуса лица, оказывающего содействие органам, осуществляющим ОРД, является их ответственность, которая содержит в себе две группы принудительных мер: меры ответственности, предусмотренные нормами актов законодательства; меры ответственности, установленные контрактом (в качестве таких мер, например, возможно установление определенных вычетов из денежных средств, предусмотренных для выплат за оказание содействия).

В таком виде статус приобретет законченную конструкцию, четко определит пределы участия лиц в решении задач ОРД, позволит сотрудникам оперативно-розыскных органов осуществлять эффективное управление действиями привлеченных к содействию лиц.

УДК 343.72

А.М. Пановицын

О ПОВЫШЕНИИ КАЧЕСТВА ОСУЩЕСТВЛЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ КРИМИНОЛОГИЧЕСКОЙ ХАРАКТЕРИСТИКИ ПРЕСТУПНИКА ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Рост числа преступлений с применением высоких технологий имеет прямую связь с интенсивным развитием процесса информатизации общества и применением компьютерных и сетевых технологий во всех ключевых областях человеческой деятельности. Как показывает статистика, личностная и психологическая характеристика правонарушителя связана с конкретным видом информации, на которую совершается преступное посягательство. Следовательно, в целях совершенствования работы по выявлению круга лиц, подозреваемых в совершении компьютерных преступлений, целесообразно классифицировать граждан по виду деяний, совершенных с компьютерной информацией. Так, к первой и самой многочисленной группе компьютерных мошенников, специализирующихся на получении разнообразных паролей пользователей интернета, хищении информации о кредитных картах, незаконном распространении программных продуктов и вредоносных программ, написании компьютерных вирусов, не содержащих сложного программного кода, получающих неправомерный доступ к информации, хранящейся в ПЭВМ, следует отнести лиц мужского пола в возрасте 14–25 лет. К данной категории преступников относятся лица из семей среднего достатка, получающие среднее (учащиеся 8–11 классов средней школы) или среднее специальное образование, связанное с компьютерными технологиями, а также студенты старших курсов или выпускники технических учреждений высшего образования, как правило, имеющие в своем распоряжении более одного персонального компьютера. Данная категория лиц обладает начальным знанием языков программирования низкого и высокого уровней и аппаратной части ПЭВМ. Мошенники в большинстве случаев увлечены компьютерами, предпочитают общение с единомышленниками, нигде не работают либо работают системными администраторами в организациях с невысоким уровнем заработной платы, общаются главным образом с использованием компьютерного сленга, смешивают русский и английский языки, небрежны, допускают массу грамматических ошибок. Большую часть времени они проводят за компьютером, в основном в интернете, к преступной деятельности приобщаются рано, не осознавая, что их деяния классифицируются статьями уголовного кодекса. Основной мотивацией совершения преступлений данной категорией лиц является стремление выделиться и самоутвердиться среди сверстников.

Вторая группа лиц склонна к совершению преступлений, в основном связанных с получением несанкционированного доступа и хищением компьютерной информации с использованием локальных вычислительных сетей. К этой категории преступников относятся лица, как правило, мужского пола в возрасте 18–25 лет, из семей со средним и выше среднего достатком, имеющие среднее специальное, незаконченное высшее или высшее техническое образование, располагающие дорогостоящими ПЭВМ. Мошенники обладают фундаментальными знаниями нескольких языков программирования и аппаратной части сетевого оборудования. Для сетевых проникновений они используют программные продукты, требующие специальных знаний и подготовки, склонны организовывать групповые хакерские атаки. Чаще всего они работают системными администраторами или специалистами в фирмах по продаже программного обеспечения или компьютерных комплектующих, неплохо зарабатывают, в меру амбициозны, преимущественно общаются с представителями своей профессии, в переписке и разговорной речи умеренно пользуются специальной терминологией. Основной мотивацией к преступной деятельности является возможность получения свободного доступа к конфиденциальной информации непосредственно в процессе обслуживания и ремонта компьютеров клиентов.

Третью группу профессиональных хакеров, специализирующихся на промышленном и техническом шпионаже, написании специальных вирусов и троянов для хищения компьютерных данных и денежных средств, составляют лица преимущественно мужского пола в возрасте 27–45 лет. Это, как правило, выходцы из семей с высоким уровнем достатка, получившие хорошее образование в технических учреждениях высшего образования на территории страны или за ее пределами, имеющие высокую квалификацию, владеющие несколькими языками программирования, знаниями в области сетевых протоколов и криптографии, постоянные участники семинаров по информационной безопасности и программированию, победители специализированных конкурсов, уравновешены, амбициозны, алчны. Часто работают главными специалистами и консультантами в крупных инновационных или финансовых компаниях как государственного, так и частного капитала. Основной мотивацией к совершению преступлений является возможность использования своих знаний и навыков для получения высокой финансовой прибыли нелегальным путем и существующим спросом на подобные услуги.

Следовательно, для повышения качественной составляющей в расследовании преступлений в сфере высоких технологий необходимо учитывать прямую связь вида похищаемой компьютерной информации с категорией лиц, совершающих преступления. Знание личностной и психологической характеристики правонарушителя позволит сузить круг лиц, подозреваемых в совершении преступлений в сфере высоких технологий, что повысит эффективность и сократит сроки раскрытия подобных преступлений.