

В.А. Милашев

ПРОТИВОПРАВНАЯ ДЕЯТЕЛЬНОСТЬ В КОМПЬЮТЕРНЫХ СЕТЯХ: ВОПРОСЫ КРИМИНАЛИСТИКИ

Чем активнее компьютерные сетевые технологии используются для решения повседневных задач, чем глубже они проникают в различные отрасли, "связывая" в единой информационной среде системы управления оборудованием, финансами, персоналом, системы принятия административно-хозяйственных решений, тем больше возникает опасностей использования этих технологий для совершения противоправных деяний.

Обеспечение информационной компьютерной безопасности стало одной из самых актуальных задач. Рассмотрением вопросов в этой области занимался ряд специалистов, в частности: Н.Г. Милославская, А.И. Толстой, Э. Коул, М. Купер, Д. Курц, Д. Ли, С. Мак-Клар, Д. Новак, С. Норткат, Д. Скембрей, М. Фирноу, К. Фредерик, Б. Хатч, Д. Чирилло и др.

Огромный опыт, накопленный в области защиты информации, должен быть сегодня ассимилирован для успешной борьбы с преступностью.

Особое значение этот опыт имеет для криминалистики как науки, изучающей противоправную деятельность и, в частности, следы, оставляемые на месте преступления в ходе его совершения. В этой связи особый интерес вызывает исследование способа совершения противоправных действий путем использования компьютерных сетевых технологий, а именно - воздействие по линии электросвязи на информацию в ЭВМ. Мы называем этот способ *удаленным воздействием*.

Изучение механизма взаимодействия компьютеров в сети, а также опасности его использования в противоправных целях поможет в познании закономерностей удаленного воздействия. Принимая во внимание, что способ совершения преступления тесно связан с такими элементами криминалистической характеристики, как субъект, орудие, предмет посягательства, результат и цель противоправной деятельности, подобные знания позволят выявить многообразие проявлений указанных элементов и их связи друг с другом и дадут возможность сформировать представление об особенностях объективной стороны преступления.

Изучение алгоритма обработки компьютером информации поможет познать процесс отражения события преступления, установить области локализации следов, особенности следовых картин при тех или иных видах противоправной деятельности и, соответственно, выработать на этой основе тактические приемы обнаружения, фиксации и изъятия следов противоправной деятельности для эффективного поиска злоумышленников.

Следы могут представить следователю информацию об источнике воздействия, способе воздействия, используемых злоумышленником орудиях и т.д.

Изучение поисково-познавательных процессов в деятельности по раскрытию, расследованию и предупреждению преступлений в сфере компьютерной информации позволит выявить типовые следственные ситуации, возникающие на различных этапах расследования и требующие соответствующих технико-технологических и тактико-методических приемов их реализации.

Полученные знания позволят выработать криминалистические рекомендации для успешного проведения расследований преступлений в сфере использования компьютерных технологий.

Характерной особенностью преступлений, совершенных путем удаленного воздействия, является фактическое отсутствие на месте совершения преступления его субъекта. Проявление его деятельности осуществляется посредством направления управляющих данных в адрес ЭВМ жертвы компьютерной информации. Эти управляющие данные вызывают изменения компьютерной информации, по которым можно судить о характере противоправных действий злоумышленника, направлении его умысла и, что наиболее ценно, могут отразить сведения об источнике удаленного воздействия.

Так как эти управляющие данные направляется злоумышленником не вообще в компьютерную сеть, а в адрес конкретного компьютера в сети, то местом преступления было бы правильно считать компьютер, обладающий уникальным сетевым адресом. Даже при удаленном воздействии, в ходе которого пострадала отдельная компьютерная сеть, непосредственному противоправному воздействию подвергаются компьютеры, обладающие конкретным сетевыми адресами.

Следами, оставляемыми на месте совершения преступления, будет являться совокупность компьютерной информации, измененной в результате действий злоумышленника. Взаимодействие компьютерной информации осуществляется по законам логики и строится на использовании логических схем. Учитывая природу таких следов и механизм их образования, мы предлагаем называть их **бинарными следами**.

Выявление закономерностей образования бинарных следов, областей их локализации в компьютере жертвы, выделение типичных элементов следовой картины конкретных видов криминальной деятельности в сети имеет большое методическое значение. С одной стороны, это предоставляет следователю и органу дознания набор отправных точек для поиска тех

или иных следов, а, с другой стороны, при обнаружении следов определенного вида обеспечивает возможность выдвижения типовой версии о расследуемом событии. Все это в целом позволяет успешно осуществлять поиск злоумышленников.

Для эффективного решения задач борьбы с сетевой противоправной деятельностью необходимо:

- активизировать научно-исследовательскую работу;
- решить вопрос подготовки специалистов;
- сформировать систему правовых механизмов, учитывающих особенности слеодообразования в компьютерной сети;
- установить единую межотраслевую терминологию для описания объектов, процессов и явлений в области компьютерной информации.

Как отмечалось на апрельской сессии 2001 года Парламентской Ассамблеи Совета Европы, дальнейшее развитие информационных технологий, без сомнения, увеличит скорость, масштаб и сложность компьютерных преступлений. Следующее поколение киберпреступников будет более квалифицированным и лучше финансируемым. Выслеживать их будет чрезвычайно тяжело.

Масштаб задач и ограниченность времени для их решения требуют обратить серьезное внимание на практику борьбы с компьютерной преступностью за рубежом и творчески перенимать накопленный многолетний опыт.

Только активная наступательная позиция российских правоохранительных органов, действующих совместно с коллегами из других стран, позволит уверенно противостоять преступлениям в сфере компьютерных технологий.