началу XXI в. достигли такого уровня развития, что сами начинают задавать новые параметры системной организации остальных структурных компонентов человеческой цивилизации – экономических, социальных, политических, духовных. В результате происходят трансформации данных элементов в соответствии с теми нормами, процедурами и правилами построения, которые определяются инфокоммуникационной сферой.

УДК 004.42

И.Д. Пацкевич, Р.В. Кислинский

ПРОТИВОДЕЙСТВИЕ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В КИБЕРНЕТИЧЕСКОМ ПРОСТРАНСТВЕ

Современный этап развития общества характеризуется бурным развитием и внедрением средств связи, вычислительной техники и новых информационных технологий практически во все сферы человеческой деятельности. Все это привело к формированию так называемого кибернетического пространства, впитавшего в себя не только общечеловеческие культурные ценности, но, к сожалению, и все присущие обществу пороки.

Так, пользователь информационной сети может свободно получить рецепты производства наркотиков, способы изготовления из доступных материалов самодельных взрывных устройств, переписать на свой компьютер порнографические изображения или мультимедийные журналы сомнительного содержания, получить полные тексты доктрин идейных руководителей нацизма и мирового терроризма, принять участие в электронной конференции хакеров, на которой обсуждаются вопросы несанкционированного проникновения в автоматизированные системы органов государственного управления, военных структур и т. п.

Основной целью интернет-преступников является обман пользователей глобальной паутины и кража конфиденциальной информации, которая используется после в личных целях преступника. В результате такой деятельности миллионы людей во всем мире несут значительные убытки каждый год.

Почти все виды компьютерных преступлений можно так или иначе предотвратить. Мировой опыт свидетельствует о том, что для решения этой задачи правоохранительные органы должны использовать различные профилактические меры, направленные на выявление и устранение причин, порождающих преступления, и условий, способствующих их совершению.

К группе мер предупреждения компьютерных преступлений, прежде всего, относятся нормы законодательства, устанавливающие уголовную ответственность за противоправные деяния в компьютерной сфере. Первым шагом в этом направлении можно считать Закон Республики Беларусь «О повышении компьютерной безопасности», а также Закон «Об информатизации». В ноябре 2010 г. в нашей стране была принята Концепция национальной безопасности Республики Беларусь. В ней сказано, что мир вступил в стадию кардинальных экономических, общественных, военно-политических и иных изменений, характеризующихся высокой интенсивностью и динамичностью. Предпринимаются попытки формирования и навязывания идеологии глобализма, призванной подменить или исказить традиционные духовно-нравственные ценности народов.

Но одних мер профилактики недостаточно. В целях обеспечения информационной безопасности в Республике Беларусь были созданы специальные органы по борьбе с киберпреступностью. Так, 21 апреля 2008 г. создан Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ). ОАЦ является государственным органом, осуществляющим регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственные секреты Республики Беларусь, или иные сведения, охраняемые в соответствии с законодательством от утечки по техническим каналам, несанкционированных и непреднамеренных воздействий.

Как дополнительные меры борьбы с преступностью в киберпространстве, в стране созданы отделы по раскрытию преступлений в сфере высоких технологий. Это современные, хорошо оснащенные, боеспособные подразделения, которые занимаются раскрытием и профилактикой преступлений против информационной безопасности, преступлений в сфере телекоммуникаций; противодействием хакерам, кардерам, а также распространению детской порнографии, кражам финансовых средств частных лиц и организаций путем использования компьютерной техники; оперативной и технической поддержкой служб правоохранительных органов при раскрытии тяжких и особо тяжких преступлений. Подразделения оснащены самыми современными техническими средствами раскрытия интернет-преступлений – как универсальным, так и специальным программным обеспечением. Универсальные программы общего назначения (информационно-поисковые системы, редакторы, электронные таблицы и т. п.) не только повышают производительность труда и эффективность работы по выявлению, раскрытию и расследованию преступлений, но и поднимают их на качественно новый уровень. Специализированные программы могут быть ориентированы на непосредственное их применение при осуще-

ствлении оперативно-розыскных мероприятий в направлении борьбы с информационной (в том числе компьютерной) преступностью.

В настоящее время существует программы, которые позволяют:

контролировать процесс попыток взлома компьютерной системы или сети;

определять индивидуальный почерк работы программиста и идентификационные характеристики разработанных им программ;

определять перечень электронных адресов и сайтов интернета, с которыми работал пользователь;

негласно регистрировать перечень программ, с которыми работает пользователь;

определять путь, а в некоторых случаях и конкретный адрес исходящей угрозы для компьютерных систем;

осуществлять негласный контроль над программистом, определяя характер разрабатываемых продуктов;

обнаруживать латентную и закодированную информации в компьютерной системе;

проводить идентификацию компьютерных систем по следам применения на различных материальных носителях информации;

осуществлять исследование следов деятельности оператора в целях его идентификации;

осуществлять диагностику устройств и систем телекоммуникаций на возможность осуществления несанкционированного доступа к ним;

исследовать материальные носители с целью поиска заданной информации;

осуществлять исследование компьютерных технологий для установления возможности решения конкретных преступных задач (крекинг, хакинг, фрикинг и т. п.);

исследовать программы ЭВМ и базы данных с целью определения их возможного предназначения для преступных действий (при наличии программных закладок, подпрограмм класса «троянский конь» и т. п.).

Поисковые программные средства могут найти широкое применение в оперативно-розыскной деятельности (непроцессуальная форма), в том числе и до возбуждения уголовного дела. Факт обнаружения объектов (программы закладок, программное обеспечение для изготовления вирусов или для осуществления взлома компьютерных сетей и т. п.) может послужить основанием для возбуждения дела и производства расследования. В процессуальной форме поисковые программные средства могут найти применение при проведении следственных действий, таких как следственный осмотр (все его виды), выемка предметов, документов и электронной почтовой корреспонденции, следственный эксперимент, выполняемый с целью опытной проверки показаний.

В оперативно-розыскной деятельности при расследовании компьютерных преступлений целесообразно применять криминологическое прогнозирование индивидуального и преступного группового поведения. Определенную информацию можно извлечь, анализируя сетевой трафик локальных и региональных компьютерных сетей. Полезную информацию могут дать и анализ платежей клиентов за телефонные услуги. Прогнозирование может успешно осуществляться в основе первичных материалов оперативного учета, так как его банки информации создаются на основе прогноза вероятности преступного поведения определенных криминогенных контингентов. Все это в совокупности является элементами методики криминологического прогнозирования, которое вплетается в оперативно-розыскные мероприятия при реализации форм оперативно-розыскной деятельности (поиск, профилактика, разработка). Естественно, вопросы моделирования и прогнозирования необходимо решать, используя современные технологии.

Таким образом, мы видим, что почти все виды компьютерных преступлений можно так или иначе предотвратить. Мировой опыт свидетельствует о том, что для решения этой задачи правоохранительные органы должны использовать не только различные профилактические меры, но и активные меры по борьбе с данными преступлениями. Профилактические меры следует воспринимать как деятельность, направленную на выявление и устранение причин, порождающих преступления, и условий, способствующих их совершению, а в целях борьбы следует создавать специальные подразделения, которые будут заниматься раскрытием интернет-преступлений. Для этого сотрудникам правоохранительных органов необходимо получить знания по основам учебных дисциплин в области кибернетики и вычислительной техники.

УДК 006.07

С.В. Пашковский

ОСНОВНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Начав обсуждение вопроса о совершенствовании законодательства в области информационной безопасности, необходимо отметить, что в рамках текущего доклада под информационной безопасностью пони-