Информационные технологии как средство совершения преступлений в отношении банковских карт

Гудов
Дмитрий Викторович,
старший преподаватель кафедры математических и естественнонаучных дисциплин Саратовского военного института внутренних войск МВД России, к.п.н., доцент, подполковник

Семёнов
Константин Петрович,
преподаватель кафедры математических и естественнонаучных дисциплин Саратовского военного института внутренних войск МВД России, к.т.н., доцент, майор

Технический прогресс способствует возникновению новых видов преступлений двумя основными путями. Во-первых, непосредственно. Вновь появившиеся технические средства и технологии используются злоумышленниками для более эффективного совершения преступлений традиционных видов. Во-вторых, опосредованно. Технический прогресс вызывает прогресс социальный, то есть возникновение принципиально новых видов общественных отношений. Новые общественные отношения означают новые права, которые могут быть нарушены. Таким образом, возникают принципиально новые способы совершения традиционных видов преступлений и принципиально новые виды преступлений, которые были раньше не то чтобы неосуществимы, но попросту немыслимы.

При возникновении новых общественных отношений первое время они законом не защищаются. Но достаточно быстро общество осознает необходимость защиты новых прав, особенно в тех случаях, когда эти права начинают стоить существенных денег. Новейшая история показывает, что от момента возникновения нового общественного отношения до момента, когда возникает более-менее единообразная юридическая практика его защиты, проходит от 5 до 8 лет.

Развитие и все более широкое распространение новых информационных и телекоммуникационных технологий определило необходимость правовой оценки ситуации и разработки организационно-правовых механизмов пресечения общественно опасного поведения (или «криминальной деятельности») в данной области.

Формирование отечественного законодательного регулирования в области информационных правоотношений прошло сложный путь. Признание обществом, а вслед за ним и законодателем факта существования информационного ресурса как реального объекта, имеющего материальное выражение, признание информации в качестве объекта гражданских прав, установление возможности признания права собственности физических и юридических лиц, государства на информацию, информационные системы, технологии и средства их обеспечения повлекло необходимость государственного реагирования в области уголовно-правовых запретов.

Анализ норм действующего УК РФ показывает, что развитие законодательного регулирования информационных правоотношений нашло в нем свое отражение, но для правильного понимания и оценки ряда предусмотренных УК РФ действий в качестве общественно опасных необходимо привлечение норм всего законодательства, регламентирующих эти действия как незаконные, неправомерные. Без ясного понимания норм, регулирующих информационные правоотношения, правоохранительные органы не имеют возможности правильно определить круг вопросов, подлежащих доказыванию, а затем и точно квалифицировать выявленные случаи преступлений. Без такого понимания невозможно и создание соответствующих методик расследования преступлений, совершенных в информационной сфере в целом. Между тем подобные методики расследования криминальной деятельности являются крайне необходимыми в практике, поскольку нередко данная разновидность деятельности является составной частью иных преступлений. Отсутствие четкого определения компьютерной преступности, единого понимания сущности этого явления значительно затрудняют определение задач правоприменительных органов в выработке единой стратегии борьбы с ней.

В разных источниках имеется несколько определений «компьютерного преступления» — от самого узкого (только три вышеупомянутых состава) до самого широкого (все дела, касающиеся компьютеров). В последнее десятилетие появилась самостоятельная наука «форензика» — компьютерная криминалистика.[1] Для целей форензики четкого определения компьютерного преступления не требуется. Компьютерным можно называть любое преступление, для раскрытия которого используются методы компьютерной криминалистики.

В зарубежной литературе и во многих официальных документах кроме/вместо «computer crime» также часто употребляется термин «cybercrime» — киберпреступность, киберпреступление. Определения этого термина разные, более широкие и более узкие.

1 Термин «forensics» является сокращенной формой «forensic science», дословно «судебная наука», то есть наука об исследовании доказательств – именно то, что в русском языке именуется криминалистикой. Соответственно, раздел криминалистики, изучающий компьютерные доказательства, называется по английски «computer forensics». При заимствовании слово сузило свое значение. Русское «форензика» означает не всякую криминалистику, а именно компьютерную.

Наиболее емким с нашей точки зрения является следующее определение: компьютерное преступление (киберпреступление) — уголовное правонарушение, для расследования которого существенным условием является применение специальных знаний в области информационных технологий [1].

Следует отметить, что основным мотивом совершения компьютерных преступлений является корысть. Антивирусные аналитики отмечают явную тенденцию к коммерциализации вредоносного ПО [2, 3]. Еще 10–15 лет назад почти все вирусы и черви создавались без явной корыстной цели, как полагают, из хулиганских побуждений или из честолюбия. А среди современных вредоносных программ большинство составляют программы, созданные для извлечения выгоды. Как современная вредоносная программа является лишь средством, технологическим элементом для криминального бизнеса, так и современный вирусописатель работает не сам по себе, а исполняет заказы других. Это может быть прямой заказ, когда вирмейкер получает техническое задание, исполняет его и отдает готовый продукт заказчику. Это может быть непрямой заказ, когда вирмейкер, зная потребности черного рынка, старается их удовлетворить своим продуктом, который затем и реализует (лицензирует пользователям) самостоятельно.

Уголовный кодекс РФ содержит три состава преступлений, называемых «преступлениями в сфере компьютерной информации»,— ст. 272, 273 и 274 (глава 28). Термин же «компьютерные преступления» с нашей точки зрения несколько шире, чем «преступления в сфере компьютерной информации». Он также охватывает те преступления, где компьютерная техника, программы, компьютерная информация и цифровые каналы связи являются орудиями совершения преступления или объектом посягательства. К таким преступлениям относятся: мошенничество с применением банковских карт (кардинг), мошенничество с выманиванием персональных данных (фишинг), незаконное пользование услугами связи и иной обман в области услуг связи (кража трафика), промышленный и иной шпионаж, когда объектом являются информационные системы, и т.д. По мере развития технологий электронных платежей, «безбумажного» документооборота и т.п. серьёзный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике. Необходимо также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надёжности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач.

Классификация компьютерных преступлений по статьям УК с научной точки зрения несостоятельна. Одни составы слишком широкие, другие слишком узкие. Например, формулировка статьи 272 охватывает и случай, когда несовершеннолетний завладевает копеечным логином на доступ в Интернет, и случай, когда иностранный шпион получает доступ к компьютеру с государственной тайной. Напротив, статья 187 УК (изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов) охватывает лишь очень незначительную часть кардерской деятельности, в то время как основная деятельность кардеров определена как мошенничество (статья 159) и причинение имущественного ущерба путем обмана или злоупотребления доверием (статья165).

С учетом опасности компьютерных преступлений в мировой практике постоянно происходит модернизация законодательства, ужесточение наказаний за подобного рода преступления, принимаются соответствующие международные соглашения. Как этот вопрос решается российским законодателем?

Точки зрения специалистов в данной области условно можно разделить на три группы [4].

1. Компьютерные преступления представляют собой самостоятельный вид преступной деятельности, который включает в себя составы преступлений.
2. Компьютерных преступлений как самостоятельного вида противоправных действий не существует, их следует рассматривать лишь как квалифицирующий признак обычных, «традиционных» преступлений». При этом компьютер при совершении преступления выступает в качестве объекта преступления, орудия преступления, средства, на котором подготавливается преступление или среды, в которой оно совершается.
3. Предлагается также весьма расширительное толкование понятия компьютерных преступлений, в соответствии с которым к ним относятся любые посягательства на связи и отношения людей, опосредующих применение и использование компьютерной техники.

Сразу оговоримся, что третий подход, на наш взгляд, является излишне расширительным, по существу, безграничным, и не может быть нами поддержан. Первый же совершенно очевиден, общедоступен и именно из-за этого широко применяется в мировой практике. Насколько перспективен такой подход? На наш взгляд, он крайне ограничен. Если следовать указанной логике, то уже сейчас необходимо вводить в УК новые составы преступлений: кибермошенничества, киберклеветы, кибершпионажа, киберподделки, киберхалатности, кибersаботажа и т.д.

Нам представляется более целесообразным второе направление, точнее два взаимосвязанных и взаимодополняющих подхода, позволяющих произвести определенную корректировку УК без его коренного пересмотра.

Во-первых, и это в значительной мере касается правоприменения, трактовать имеющиеся статьи УК, термины и понятия в соответствии с современным пониманием (с точки зрения информационных технологий), закрепленных в ряде федеральных законов РФ [5–8].

Во-вторых, расширить в ряде случаев квалифицирующие признаки преступлений путем включения в них определения: «с использованием современных компьютерных технологий» (в тех случаях, когда их применение явно повышает общественную опасность конкретного вида преступления).

В заключение следует еще раз подчеркнуть, что существуют весьма специфические компьютерные преступления, которые вообще не нашли своего отражения в Уголовном кодексе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Расследование преступлений в сфере информации и компьютерных технологий. Курс лекций — /Коллект. авторов под ред. проф. Черкасова В. Н.— Саратов: СЮИ МВД РФ, 2008, ISBN 5-7485-0503-1
2. Никитина Ю. Компьютерный вирус — бизнес, а не шутка (Электронный ресурс, URL: http://www.fontanka.ru, дата публикации: 26.06.2010).
3. Казимирко-Кириллова А. Киберпреступность угрожает современному бизнесу (Электронный ресурс, URL http://www.TPP-inform.ru, дата публикации 10.12.2010).
4. Черкасов В. Н. Информационные технологии и организованная преступность (Электронный ресурс, URL: http://www.crime-research.ru/library/Cherkas03.html, дата обращения: май 2011 г.).
5. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (принят ГД ФС РФ 08.07.2006) // Собрание законодательства РФ», 31.07.2006, N 31 (1 ч.), ст. 3448.
6. Федеральный закон от 10.01.2002 N 1-ФЗ «Об электронной цифровой подписи» (принят ГД ФС РФ 13.12.2001)// Российская газета, N 6, 12.01.2002.
7. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне» (принят ГД ФС РФ 09.07.2004)// Российская газета, N 166, 05.08.2004.
8. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» (принят ГД ФС РФ 08.07.2006)// Российская газета, N 165, 29.07.2006.