ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В УК РОСИЙСКОЙ ФЕДЕРАЦИИ

А.И. Коробеев
доктор юридических наук, профессор
заслуженный деятель науки Российской Федерации
(Дальневосточный Федеральный университет, Владивосток)

Бурное развитие в последнее время в мире коммуникационных систем с использованием для распространения информации компьютерной техники привело к появлению новых общественных отношений, нуждающихся в уголовно-правовой защите. Законодатель России в главе 28 УК РФ криминализировал наиболее опасные виды посягательств на эти отношения. К ним относятся: а) неправомерный доступ к компьютерной информации (ст. 272 УК); б) создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК); в) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 247 УК).

Отсюда видно, что далеко не все деяния, именуемые в литературе киберпреступлениями (преступлениями в киберпространстве), интернет-преступлениями, компьютерными преступлениями (например, компьютерное мошенничество) охватываются понятием „преступления в сфере компьютерной информации". Таковыми признаются лишь предусмотренные уголовным законом и совершаемые виновно общественно опасные деяния, посягающие на общественные отношения в сфере обеспечения безопасности компьютерной информации.

Рассматриваемые преступления в соответствии с Конвенцией о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.) относятся к категории „преступлений против конфиденциальности, целостности и доступности компьютерных данных".

Видовым объектом этих преступлений выступают отношения, связанные с обеспечением конфиденциальности, целостности и доступности компьютерной информации, а также сохранности и неприкосновенности средств ее хранения, обработки и передачи.

Предметом преступления служат компьютерная информация; средства хранения, обработки или передачи компьютерной информации; информационно-телекоммуникационные сети; оконечное оборудование.

Что касается самих средств хранения, обработки и передачи компьютерной информации, то ими являются ее материальные носители: дискеты, жесткие диски, оптические диски, USB – флешнакопители, карты памяти и др. Инструментом обработки служит компьютер, т.е. электронное устройство, предназначенное для автоматической обработки информации путем выполнения заданий, определенных последовательностью операций. Имеется в виду не только персональный компьютер с обычным набором аппаратных средств (материнская плата, блок питания, жесткий диск, устройства ввода и вывода информации и т.д.), но и любой прибор, обрабатывающий

цифровую информацию (мобильный телефон, цифровой фотоаппарат, контрольно-кассовая машина и др.), а также аналоговый аппарат (например, автопилот). [1]

В соответствии со ст. 2 Федерального закона РФ от 27 июля 2006 г. № 149 – ФЗ „Об информации, информационных технологиях и о защите информации"[2] информационно-телекоммуникационная сеть есть технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Согласно ст. 2 Федерального закона от 7 июля 2003 г. № 126 – ФЗ „О связи", оконечное (пользовательское) оборудование – это технические средства для передачи и (или) приема сигналов электросвязи по линиям связи[3], подключенные к абонентским линиям и находящиеся в пользовании абонентов или предназначенные для таких целей.

С объективной стороны преступления в сфере компьютерной информации могу выражаться в форме как действий (ст.ст. 272, 273 УК), так и бездействия (ст. 274 УК). Все составы (кроме деяния, предусмотренного ч. 1 ст. 273 УК) – *материальные. Последствиями* в основных составах компьютерных преступлений выступают уничтожение, блокирование, модификация, копирование компьютерной информации, крупный ущерб.

Уничтожение компьютерной информации означает приведение ее полностью в непригодное для использования по своему функциональному назначению состояние (например, стирание ее с жесткого диска).

Блокирование информации предполагает создание препятствий к свободному доступу к информации при сохранении самой информации. *Модификацией* информации признается внесение любых изменений в исходную информацию без согласия на то ее собственника или владельца. *Копирование* информации есть ее тиражирование (дублирование), т.е. воспроизводство информации в любой материальной форме. *Крупным ущербом* в статьях о преступлениях в сфере компьютерной информации считается ущерб, сумма которого превышает один миллион рублей.

С *субъективной стороны* лишь создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК) предполагает только умышленную форму вины. Остальные компьютерные преступления могут совершаться как с умыслом, так и по неосторожности.

Субъектом преступлений, предусмотренных ст.ст. 272, 273 УК, является любое физическое вменяемое лицо, достигшее 16-летнего возраста. *Субъект* преступления, предусмотренного ст. 274 УК, – специальный. Им может быть только лицо, на которое возложена обязанность соблюдать правила эксплуатации средств хранения, обработки, передачи компьютерной информации, информационно-телекоммуникационных сетей или оконечного оборудования.

Квалифицированными и *особо квалифицированными* видами компьютерных преступлений выступают те же деяния, совершенные из корыстной заинтересованности, группой лиц по предварительному сговору, организованной группой, лицом с использованием своего служебного положения, с причинением тяжких последствий или созданием угрозы их наступления.

С момента введения в УК РФ 1996 г. самостоятельной главы 28 „Преступления в сфере компьютерной информации" и до самого последнего времени одной из

[1] См.: Уголовное право. Особенная часть: учебник для бакалавров/ под ред. А.И. Чучаева. – М.: Проспект, 2012. С. 349.
[2] СЗ РФ. 2006. № 31 (ч. 1). Ст. 34-48.
[3] СЗ РФ. 2003. № 28. Ст. 28-95.

достаточно серьезных оставалась проблема использования в ней устаревшей терминологии. Лишь с принятием Федерального закона РФ от 7 декабря 2011 г. из диспозиций всех норм, входящих в данную главу, и их названий исключен термин „электронно-вычислительная машина (ЭВМ)". Тем самым сфера возможного применения соответствующих норм заметно расширилась. Существенно изменилась и редакция упомянутых норм. Так, в ст. 272 УК появилось примечание, согласно которому компьютерная информация стала трактоваться как сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Отсюда возникла проблема, суть которой сводится к следующему. Любые сигналы, как правило, теснейшим образом связаны с носителями информации и средствами их хранения. В зависимости от носителя информации сигналы могут быть электрическими, электромагнитными, оптическими и т.д. В уголовном же законе речь идет только об электрических сигналах. Между тем информация лишь в момент обработки и ее конечной передачи на компьютер преобразуется в электрический сигнал. В этой связи в теории уголовного права законодателю небезосновательно предложено уточнить формулировку данной статьи, назвав электрический сигнал „конечным", т.е. уже поступившим в вычислительное устройство.

С другой проблемой судебная практика может столкнуться в процессе применения ст. 273 УК. Прежняя редакция упомянутой нормы предусматривала в качестве вредоносных программ только такие программы, которые заведомо приводили к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. Таким образом, уголовный закон боролся с неправомерной деятельностью достаточно ограниченного круга лиц, работающих на „профессиональной" основе (хакеров, компьютерных мошенников и т.д.).

Новая редакция ст. 273 УК позволяет вовлечь в орбиту уголовно-правовых отношений практически любого пользователя нелицензированного программного обеспечения. Дело в том, что данная статья в нынешнем ее виде приравняла к вредоносным компьютерным программам и те программы, которые предназначены для нейтрализации средств защиты компьютерной информации. Отсюда вредоносными программами могут теперь считаться все так называемые „патчи", „кейгены", „кряки" и подобное программное обеспечение, изначально призванное нейтрализовать средства защиты[4].

К уголовной ответственности по ст. 273 УК могут привлекаться не только создатели и распространители „варезного" софта (что имело место и ранее), но и рядовые пользователи, каковыми являются представители большей части российского компьютерного сообщества. В соответствии же с положениями постановления Пленума Верховного Суда РФ от 26 апреля 2007 г. „О практике рассмотрения судами уголовных дел о нарушениях авторских, смежных, изобретательских и патентных прав, а также о незаконном использовании товарного знака" сбытчиками (распространителями) вредоносного программного обеспечения в виде „незарегистрированного софта" будут считаться лица, оказывающие содействие в его распространении, например, путем размещения гиперактивной ссылки на ресурс, где осуществляется

[4] См.: *Гаврилов В.М.* Противодействие преступлениям, совершенным в сфере компьютерной и мобильной коммуникаций организованными преступными группами. Саратов, 2009. С. 20-28; *Кузнецов А.П., Маршакова Н.Н., Паршин С.М.* Преступления в сфере компьютерной информации. Нижний Новгород, 2008. С. 21-25.

физическое хранение файла. С учетом наработанной в правоохранительных органах практики вычислить лицо, разместившее ссылку на „взломанный софт", и привлечь его к уголовной ответственности не составит особой сложности[5].

Одним из проблемных в процессе квалификации компьютерных преступлений является вопрос об отграничении этих преступлений от смежных преступных деяний. В частности, возникает вопрос: правомерно ли пиратское тиражирование компьютерных программ квалифицировать только по ст. 146 УК, а хищение денежных средств с использованием компьютерных сетей – только по ст. ст. 158 и 159 УК? Или в этих случаях требуется дополнительная квалификация еще и по статьям об ответственности за компьютерные преступления?

Мнения ученых по этому поводу разделились. Одни из них полагают, что компьютер в подобных ситуациях является только средством, техническим инструментом совершения соответствующих преступлений, а поэтому квалификация по совокупности исключается[6]. Другие авторы настаивают на необходимости дополнительного инкриминирования компьютерных преступлений[7].

Нам представляется, что в описанных выше ситуациях мы сталкиваемся с идеальной совокупностью преступлений. При хищении безналичных денег с помощью компьютера путем неправомерного доступа к охраняемой законом компьютерной информации с последующей модификацией или копированием этой информации злоумышленник не только посягает на отношения собственности, но и одновременно причиняет вред другой группе общественных отношений, связанных с обеспечением конфиденциальности охраняемой компьютерной информации. В результате мы имеем идеальную совокупность преступлений против собственности (ст. ст. 158 и 159 УК) и в сфере компьютерной информации (ст. 272 УК). Ту же совокупность можно обнаружить и в случае нарушения авторских прав путем сбыта контрафактных экземпляров произведений, полученных в процессе неправомерного доступа к охраняемой компьютерной информации. Дополнительным аргументом в пользу такой квалификации может служить следующая аналогия. В случае совершения разбойного нападения с применением оружия требуется квалификация по совокупности преступлений, предусмотренных ст. ст. 162 и 222 УК, поскольку в данном случае страдает еще один объект – отношения общественной безопасности (п. 23 постановления Пленума Верховного Суда РФ от 27 декабря 2002 г. „О судебной практике по делам о краже, грабеже, разбое").

Таким образом, при совершении с помощью компьютерной техники преступлений, посягающих на разные объекты, требуется квалификация по совокупности этих преступлений.

---

[5] См.: *Батурин Ю.М., Жодзинский А.М.* Компьютерная преступность и компьютерная безопасность. М., 2011. С. 135.

[6] См.: *Тропина Т.Л.* Киберпреступность. Понятие, состояние, уголовно-правовые меры борьбы. Владивосток, 2009. С. 191-193.

[7] См.: *Ляпунов Ю., Максимов В.* Ответственность за компьютерные преступления // Законность. 2009. № 1. С. 19.