УДК 025.4.03:34

ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В УГОЛОВНОМ КОДЕКСЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

А.Н. Ягудин, адъюнкт кафедры уголовного права Казанского юридического института МВД России

Сегодня компьютеры занимают одно из важнейших мест в жизни и деятельности как отдельного человека, так и организаций, крупных и мелких предприятий, а также государства в целом.

Не трудно заметить, что еще совсем недавно все, что связано с ЭВМ (компьютерами), было непривычным для широких слоев населения России.

Современный персональный компьютер сильно отличается от предшествующих крупногабаритных компьютеров по множеству параметров. Так, если для размещения (вместе с периферийным оборудованием) ставших ныне достоянием истории ЭВМ требовались большие площади, то их миниатюрным потомкам найдется место практически в каждой квартире.

Но сейчас изменилась и сфера применения компьютера – границы ее заметно расширились. Теперь компьютер – это не только обучающая игрушка и печатная машинка. С каждым днем во всем мире увеличивается число пользователей всемирной компьютерной сети Интернет. Несмотря на определенную техническую отсталость России, темпы интеграции сети Интернет всей страны настолько велики, что трудно делать какие-либо прогнозы, касающиеся перспектив этого явления.

Однако вместе с положительными тенденциями технического прогресса имеются и негативные. Продолжающийся во всем мире процесс компьютеризации различных сфер жизни порождает нежелательные явления, которые до настоящего времени не до конца поняты и изучены. Так, многие проблемы обусловлены медико-психологическими факторами, сопряжены с этическими и нравственными, а также некоторыми другими аспектами.

Главной проблемой компьютеризации в настоящее время становится распространение компьютерных преступлений.

Одной из причин их возникновения явилось информационно-технологическое оснащение предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных. Второй причиной стала реальная возможность получения значительной экономической выгоды в результате противоправных деяний с использованием ЭВМ.

Опасность компьютерных преступлений состоит в том, что уничтожение, блокирование, модификация информации, важной для действий, связанных с управляющими датчиками сложных компьютерных систем оборонного и производственного назначения, способны повлечь гибель людей, причинить вред их здоровью, уничтожить имущество в больших размерах.

В Российской Федерации компьютерная преступность имеет высокую степень латентности в связи с общей криминогенной обстановкой и отсутствием до недавнего времени соответствующих норм уголовного законодательства, а также специфичностью самой компьютерной сферы, требующей специальных

познаний. Сложившаяся ситуация определила необходимость принятия норм уголовного закона, предусматривающих ответственность за совершение преступлений в сфере компьютерной информации. Так, в Уголовном кодексе Российской Федерации 1996 года (далее – УК РФ) появилась глава 28 «Преступления в сфере компьютерной информации», которая включает три статьи: «Неправомерный доступ к компьютерной информации» (статья 272), «Создание, использование и распространение вредоносных программ для ЭВМ» (статья 273), «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» (статья 274).

Для изучения преступлений, предусмотренных главой 28 УК РФ, используются термины, взятые из технических наук, которые применяются законодателем и учеными. Так, среди них можно выделить такие понятия, как «база данных» (поименная совокупность структурированных данных, относящихся к определенной предметной области), «вычислительная техника» (совокупность технических и материальных средств (ЭВМ, устройства, приборы, программы и др.), предназначенные и используемые для автоматизации процессов обработки информации), «данные» (информация, представленная в формализованном виде, пригодном для введения ее в ЭВМ и последующей автоматизированной обработки), «информация» (совокупность данных, сведений, фактов, циркулирующих в информационных процессах, в каналах прямой и обратной связи), «программа» (последовательность указаний (команд) для ввода исходных данных, их обработки и выдачи результатов для реализации алгоритма задачи), «система ЭВМ» (ряд программно совместимых ЭВМ, имеющих одинаковую архитектуру (совокупность основных устройств, узлов и блоков ЭВМ). Система ЭВМ образует компьютерную (вычислительную, информационную) сеть.

Общим объектом названных преступлений являются общественные отношения в сфере обеспечения информационной безопасности, а к непосредственным объектам преступного посягательства относятся базы и банки данных конкретных компьютерных систем или сетей, их отдельные файлы, а также компьютерные технологии и программные средства их обеспечения, включая средства защиты компьютерной информации.

Согласно статье 272 УК РФ уголовная ответственность за неправомерный доступ к компьютерной информации наступает, если это деяние повлекло за собой либо уничтожение, блокирование, модификацию, либо копирование информации, либо нарушение работы ЭВМ или их сети.

Ответственность по части первой статьи 273 УК РФ предусматривается вне зависимости от наступления общественно опасных последствий. Она предусмотрена за сам факт совершения одного из следующих действий:

а) создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети;

б) использование либо распространение таких программ или машинных носителей с такими программами.

В случае если одно из описанных действий повлечет тяжкие последствия, применяется часть вторая статьи 273 УК РФ, предусматривающая более строгое наказание.

Огромный вред наносят нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети. Это может привести не только к сбоям в работе оборудования, но в некоторых случаях и полностью парализовать работу предприятия, учреждения или организации. Поэтому законодательно установлено, что в случае причинения существенного вреда в результате указанных действий, а также при наступлении по неосторожности тяжких последствий эти деяния наказуемы в уголовном порядке, если они повлекли уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ (статья 274 УК РФ).

Достаточную сложность вызывают вопросы квалификации перечисленных деяний, поэтому даже в кратком обзоре нельзя обойти вниманием неко-

торые наиболее сложные и в то же время важные для правильной юридической оценки деяния аспекты.

В соответствии с этим значимым представляется уяснение смысла понятий и положений, недостаточно четко или неоднозначно сформулированных в законе.

Так, употребляемые в тексте статьи 272 УК РФ словосочетания «неправомерный доступ» и «служебное положение», а также предусмотренное в статьях 273 и 274 УК РФ квалифицирующее обстоятельство «тяжкие последствия» подлежат конкретизации.

В части первой статьи 272 УК РФ речь идет о неправомерном доступе к компьютерной информации, охраняемой законом. Таким образом, наказуем доступ не к любой информации, а только к законодательно защищенной. В то же время неправомерность – это не обязательно нарушение закона. Понятие неправомерности шире понятия незаконности. С другой стороны, нельзя рассматривать неправомерность как любой без исключения случай нарушения установленного порядка доступа к охраняемой законом информации. Следует согласиться с мнением о том, что доступ к информации неправомерен, если лицо не имело права вызывать ее, знакомиться с ней, а тем более распоряжаться ею. Среди способов совершения такого доступа можно назвать: использование чужого имени, изменение физического адреса технического устройства, подбор пароля, нахождение и использование «пробелов» в программе, любой другой обман системы защиты информации.

Совершение деяния, указанного в части первой статьи 272 УК РФ, специальным субъектом (лицом с использованием своего служебного положения) предусмотрено в качестве квалифицированного состава.

Законодатель под специальным субъектом понимает отдельных лиц, занимающих соответствующие руководящие должности в сфере применения компьютерной техники, а также программистов, операторов ЭВМ, наладчиков оборудования и т.д. Однако неконкретизированность формулировок уголовного закона, отсутствие в нем толкования понятия «служебное положение» не позволяют однозначно утверждать, что речь идет о статусе лица по месту работы, сопряженном исключительно с использованием компьютерной техники. Рассматриваемое квалифицирующее обстоятельство должно толковаться шире. В частности, так должно расцениваться использование лицом своих властных или иных служебных полномочий, форменной одежды и атрибутов, служебных удостоверений, а равно сведений, которыми оно располагает в связи со своим служебным положением.

Эффективность норм о преступных посягательствах в сфере компьютерной информации значительно снижается из-за оценочного характера понятия тяжких последствий. На практике его содержание определяется в каждом конкретном случае с учетом всей совокупности обстоятельств дела. Разумеется, к тяжким последствиям следует относить, например, причинение крупного материального ущерба, серьезное нарушение деятельности предприятий, организаций и учреждений, наступление аварий и катастроф, причинение вреда здоровью людей.

Однако даже в случае привлечения к оценке тяжести причиненного вреда специалистов и экспертов она в конечном счете определяется усмотрением судебно-следственных органов, а не буквой закона.

Закрепленные в статьях 272–274 УК РФ нормы не охватывают всего спектра общественно опасных деяний, условно называемых компьютерными преступлениями. Например, ответственность по статье 274 УК РФ предусмотрена лишь за действия, вызвавшие неблагоприятные последствия по неосторожности. Умышленные же деяния, направленные на нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети именно с целью причинения тяжких последствий, не охватываются содержанием статьи 274 УК РФ. Это лишь способ совершения другого преступления. Оно будет квалифицироваться с учетом наступивших последствий по совокупности с преступлением, предусмотренным названной статьей УК РФ. Представляется, что такое деяние также можно отнести к категории компьютерных преступлений.

Компьютерными называют также

те преступления, в которых компьютер рассматривается как техническое средство совершения преступления. Подчеркиваем, именно техническое средство с его специфическими техническими возможностями, а не просто орудие преступление.

Нельзя также признать правильным причисление к категории компьютерных преступлений всех случаев, когда компьютер является предметом посягательства. В описанных составах, предусмотренных статьями 272–274 УК РФ, компьютер как предмет посягательства может расцениваться лишь с определенной долей условности. Условность заключается в том, что он рассматривается в этом случае не просто как предмет материального мира, а как совокупность информационных и аппаратных структур. Предметом же преступления в уголовном праве признается вещь (предмет объективного материального мира), по поводу которой совершается преступление.

Например, при совершении кражи чужого имущества (статья 158 УК РФ) непосредственным объектом могут являться отношения личной собственности, на которые посягает преступник, а роль предмета преступления могут играть автомашина, компьютер, личные вещи, которыми завладевает преступник. Предметом хищения и иных преступлений, ответственность за совершение которых предусмотрена нормами соответствующей главы УК РФ, является чужое, т.е. не находящееся в собственности или законном владении виновного, имущество. Следовательно, если по обстоятельствам дела компьютер является просто вещью, по поводу которой совершается преступление, то такое деяние не может быть отнесено к числу компьютерных преступлений. Таким образом, если компьютерная аппаратура представляет собой предмет преступления против собственности, ее хищение, уничтожение или повреждение надлежит квалифицировать по статьям 158–168 УК РФ.

Предмет преступления следует отличать от орудий и средств совершения преступления. Эти понятия используют, когда требуется указать, с помощью чего (приспособлений, приемов) совершается преступление. Один и тот же предмет материального мира в одном преступлении может играть роль предмета преступления (например, пистолет при его краже), а в другом являться орудием преступления (когда похищенный пистолет использован при вооруженном нападении). Компьютер как техническое средство совершения преступления рассматривается в ряду с такими средствами, как оружие, транспортное средство, любое техническое приспособление. В этом смысле его использование имеет прикладное значение, например, для хищения, сокрытия налогов и т.д. Такого рода действия не рассматриваются в качестве самостоятельных преступлений, а квалифицируются по различным статьям УК.

Таким образом, в компьютерных преступлениях практически невозможно выделить единый объект преступного посягательства. Налицо также множественность предметов преступных посягательств с точки зрения их уголовно-правовой охраны. Представляется, что к рассматриваемой категории преступлений могут быть отнесены только противозаконные действия в сфере автоматизированной обработки информации. Иными словами, объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер служит орудием посягательства.

Действующим российским уголовным законодательством достаточно подробно регламентирована ответственность и наказуемость деяний в рассматриваемой сфере. Уже сам факт уголовно-правовой защиты общественных отношений, регулирующих изготовление, использование, распространение и защиту компьютерной информации, имеет профилактическое значение.

Однако анализ текста закона позволяет констатировать, что ситуация все-таки не совсем благополучна. То, что криминализированы некоторые общественно опасные деяния в сфере компьютерной информации, разумеется, в определенной мере поможет предотвратить или значительно ослабить их негативное влияние. Но процесс совершенствования уголовного законодательства не должен останавливаться. Обусловлено это тем, что компьютерная преступность не знает границ. Все-

мирная компьютерная сеть Интернет позволяет электронно-вычислительным системам, находящимся в различных точках земного шара, взаимодействовать друг с другом.

Практически любой человек, имея компьютер и модем, при наличии телефонной линии может, не покидая удобной квартиры, отправиться в виртуальное путешествие, сделать необходимые покупки, наконец, произвести банковские операции. Но «всемирная паутина» облегчила жизнь не только правопослушных граждан. Свою выгоду извлекают также представители криминального мира.

Нет нужды цитировать сообщения о конкретных случаях несанкционированного проникновения в государственные или частные банки данных, а также о других криминальных фактах такого рода. Каждое подобное происшествие при наличии комплекса уголовно-процессуальных доказательств может быть квалифицировано по одной или нескольким статьям Уголовного кодекса. Об этом вкратце уже было сказано. Но существует проблема, которая пока не привлекает к себе широкого внимания, хотя при определенных обстоятельствах она может произвести эффект разорвавшейся бомбы.

Так, в случае противоправного использования возможностей компьютерной техники и современных средств связи уже сейчас достаточно трудно юридически верно определить место совершения преступления. С учетом существующих технических возможностей и тенденций развития преступного мира можно прогнозировать осложнение ситуации. Представляется, что место расположения ЭВМ, с помощью которой злоумышленник совершает посягательство, крайне редко будет совпадать с местом расположения объекта посягательства.

Кроме того, для уголовно-правовой квалификации деяний иногда значимо место, где наступили вредные последствия общественно опасного деяния. Если объектом посягательства явилась компьютерная информация, то преступные последствия деяния, в свою очередь, могут наступить в месте, отличном от места хранения этой информации. С учетом возможностей, предоставляемых компьютерными сетями, нельзя исключить, что преступные последствия наступят либо в какой-то конкретной и единственной точке земного шара, либо на территории нескольких государств, либо на территории всех государств, имеющих доступ в сеть.

Вследствие этих обстоятельств особое значение приобретает правильное решение вопроса о пределах действия уголовного закона в пространстве.

Действие уголовного закона в пространстве определено взаимосвязанными принципами территориальности (статья 11 УК РФ) и гражданства (статья 12 УК РФ). Поскольку преступление всегда совершается каким-либо лицом на какой-либо территории, оба названных принципа действуют одновременно. Согласно основанному на незыблемости суверенитета России принципу территориальности все лица, совершившие преступления на территории Российской Федерации, подлежат уголовной ответственности по УК РФ (статья 11 УК). Преступления, совершенные в пределах территориальных вод или воздушного пространства Российской Федерации, признаются совершенными на территории Российской Федерации. Действие УК РФ распространяется также на преступления, совершенные на континентальном шельфе и в исключительной экономической зоне Российской Федерации.

Уголовным законом определено, каким образом должны быть квалифицированы деяния, совершенные в открытом водном или воздушном пространстве вне пределов России. На международном уровне закреплена даже юрисдикция космических аппаратов. В то же время в регламентации уголовной ответственности за совершение деяний с использованием компьютерных сетей налицо пробел законодательства.