НЕПОСРЕДСТВЕННЫЙ ОБЪЕКТ СОСТАВА ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТ. 274 УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ

© 2011 А.Н. Ягудин
Казанский юридический институт Министерства внутренних дел Российской Федерации
E-mail: Adel.Yagudin@gmail.com

Статья посвящена проблемам определения непосредственного объекта состава преступления, предусмотренного ст. 274 Уголовного кодекса Российской Федерации, устанавливающей ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Рассматриваются и сравниваются мнения различных авторов по этому вопросу. Предлагается совершенствовать российское законодательство путем введения термина "компьютерная информация".

Ключевые слова: статья 274 УК РФ, ЭВМ, незаконная эксплуатация системы ЭВМ или их сети, гл. 28 УК РФ, компьютерная информация.

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, несанкционированные действия по незаконному вмешательству в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям. Опасность преступлений, при которых используются компьютеры, многократно возрастает, когда они совершаются в отношении функционирования объектов жизнеобеспечения, транспортных и оборонных систем, атомной энергетики.

Правовое регулирование в области функционирования ЭВМ, информатизации и информационных ресурсов осуществляется различными отраслями права (гражданским, авторским, административным и т.д.). Вместе с тем степень и распространенность компьютеризации в нашем обществе достигли такого уровня, когда общественные отношения в данной сфере объективно требуют и уголовно-правового регулирования. Поэтому закономерным стало появление в Особенной части Уголовного кодекса Российской Федерации (УК РФ) отдельной главы, в которой предусмотрены нормы, связанные с преступлениями в сфере компьютерной информации. Введение в Уголовный кодекс ст. 272-274 свидетельствует о стремлении законодателя не только обеспечить уголовно-правовое регулирование новой сферы общественных отношений, но и путем угрозы уголовным наказанием максимально снизить негативные издержки неправомерного или недобросовестного обращения с ЭВМ и компьютерной информацией.

В литературе утверждается, что в век компьютерных технологий гораздо легче нанести вред, используя клавиатуру и мышь, нежели взрывное устройство. Несмотря на некоторую гипертрофированность этого утверждения, можно согласиться, что компьютерные преступления причиняют большой вред экономикам развитых стран. С появлением персональных электронных вычислительных машин (ПЭВМ), а равно и персональных компьютеров пользователи получили неограниченные возможности выбирать программное обеспечение для своей ПЭВМ в зависимости от характера решаемых с ее помощью задач. Одновременно с этим начали совершаться разнообразные правонарушения в данной сфере. Так, в США первое компьютерное преступление было зафиксировано еще в 1966 г., а в бывшем СССР - в 1979 г. Оно было совершено в г. Вильнюсе, представляло собой хищение 78 574 руб. и удостоилось занесения в международный реестр подобных правонарушений.

Родовым объектом компьютерных преступлений являются общественные отношения в сфере экономики. Глава 28 УК РФ называется "Преступления в сфере компьютерной информации", но большинство авторов в качестве видового объекта компьютерных преступлений называют общественные отношения, связанные с безопасностью компьютерной информации.

Более широким термином по сравнению с безопасностью компьютерной информации является "информационная безопасность". Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства (ст.1 Доктрины информационной безопасности Российской Федерации, утвержденной Президентом РФ 9 сентября 2000 г. № Пр-1895).

Следует отметить, что значительный объем исследований по проблематике обеспечения информационной безопасности выполнен в естественных и технических науках, в рамках которых разрабатываются методы криптографии, теории защиты информации и безопасности информационных систем. Интенсивно развивается направление технических наук, связанное с защитой информации в информационных и телекоммуникационных системах от несанкционированного доступа. Интенсифицируются исследования проблем обеспечения информационной безопасности в политологии, социологии и психологии. Определенные научные результаты получены и в юридической науке. Для настоящего исследования имеет значение уголовно-правовой аспект информационной безопасности.

В основе содержания понятия информационной безопасности лежит понятие безопасности. Безопасность представляет собой сложное социально-политическое явление, и его изучением занимаются специалисты, работающие в разных отраслях науки. А.А. Стрельцов полагает, что безопасность есть невозможность нанесения вреда кому-нибудь или чему-нибудь вследствие проявления угроз, т.е. их защищенность от угроз. Однако безопасность не всегда обеспечивается только защитой. Она может быть также достигнута, как отмечается в литературе, соответствующими правилами поведения и взаимодействия объектов, высокой профессиональной подготовкой персонала, надежностью всех видов обеспечения функционирования объектов информационной безопасности и т.д.

Среди других видов безопасности информационная безопасность обладает наибольшей степенью неопределенности. Это связано с ее существенными свойствами, вытекающими из глобальности самой информации, разнообразия форм и видов информации и ее носителей, наличия информационного аспекта во всех видах человеческой деятельности.

Таким образом, основное содержание понятия информационной безопасности заключается в состоянии защищенности жизненно важных интересов различных субъектов в информационной сфере на сбалансированной основе от внутренних и внешних угроз.

Некоторые авторы стараются занять обособленную позицию в определении видового объекта преступлений в сфере компьютерной информации. Так, по мнению В.А. Колобова и В.Н. Ясенева, компьютерные преступления направлены против установленного порядка общественных отношений, который регулирует изготовление, использование, распространение и защиту компьютерной информации.

Аналогичного мнения придерживаются авторы одного из комментариев к УК РФ, выделяя отношения по производству, хранению, использованию, распространению или защите информации и информационных ресурсов в качестве видового объекта.

По мнению других, компьютерные преступления - это отношения по безопасности использования компьютерной информации. Так, В.Ю. Максимов полагает, что их объектом выступают отношения по нормальному, безопасному использованию компьютерной информации.

В. Лосев определяет как видовой объект компьютерных преступлений информационную безопасность. Под информационной безопасностью понимается совокупность общественных отношений, складывающихся в процессе защиты информационных ресурсов и охраны прав субъектов информатизации, а также обеспечения безопасности пользователей и пользования компьютерными системами и сетями.

Т.Г. Смирнова также считает, что видовым объектом рассматриваемой группы преступлений выступает информационная безопасность. Под ней понимается специфическая группа общественных отношений, содержание которой составляют права и интересы различных субъектов в области обеспечения безопасности использования информации и информационных ресурсов, необходимых для нормальной жизнедеятельности социума.

И наконец, есть позиция, согласно которой родовым объектом рассматриваемой группы преступлений является не информационная, а компьютерная безопасность.

Таким образом, видовым объектом преступлений в сфере компьютерной информации следует признать общественные отношения, связанные с безопасностью компьютерной информации.

Непосредственным объектом преступления, предусмотренного ст. 272 УК РФ, являются общественные отношения в сфере охраны компьютерной информации. Объектом создания, использования и распространения вредоносных программ для ЭВМ выступают общественные отношения в сфере обеспечения компьютерной безопасности.

В научной литературе непосредственный объект преступления, предусмотренного ст. 274 УК РФ, определяется по-разному.

Так, Ю.В. Гаврилин считает, что непосредственным объектом анализируемого преступления являются общественные отношения в сфере соблюдения установленных правил, обеспечивающих нормальную эксплуатацию ЭВМ, системы ЭВМ или их сети. Дополнительный объект нарушения правил эксплуатации ЭВМ, их системы или сети факультативен. Его наличие зависит от вида вреда, причиненного правам и законным интересам потерпевшего. Дополнительным объектом может, например, выступать право собственности, авторское право, право на неприкосновенность частной жизни, личную и семейную тайну, общественные отношения по охране окружающей среды, внешняя безопасность Российской Федерации и др.

С таким определением непосредственного объекта согласиться нельзя. Статья 274 УК действительно предусматривает ответственность за нарушение правил и является бланкетной, но это не означает, что объектом следует признать общественные отношения в сфере нарушения правил. Тогда мы и объектом ст. 264 УК должны признавать отношения в сфере нарушения правил. Но там непосредственным объектом являются отношения, связанные с безопасностью дорожного движения.

Что касается дополнительного непосредственного объекта, то им не могут быть объекты других преступлений, как то право на неприкосновенность частной жизни, поскольку за вред таким объектам виновный будет отвечать отдельно и деяние следует в таком случае квалифицировать по совокупности преступлений.

Но все же дополнительный объект присутствует, на это указывает упоминание в диспозиции ст. 274 существенного вреда. Таким объектом могут выступать отношения собственности, если был нанесен имущественный ущерб, или отношения, связанные с нормальным функционированием организации или государственного органа.

А.Б. Борисов считает, что непосредственным объектом рассматриваемого преступления являются имущественные и личные неимущественные права на информацию.

А.В. Наумов непосредственным объектом называет компьютерную безопасность в сфере эксплуатации ЭВМ, системы ЭВМ и их сети.

Представляется, что непосредственным объектом преступления, предусмотренного ст. 274 УК РФ, являются отношения, связанные с безопасностью компьютерной техники и ее сети.

Многие авторы называют в качестве предмета преступлений, предусмотренных ст. 272 и 274 УК РФ, компьютерную информацию.

В то же время професоор В.С. Комиссаров отмечает, что информационная структура (программа, информация), которая содержится в компьютере, не может являться предметом данной группы преступлений, поскольку машинная информация не отвечает одному из основных критериев предмета преступлений против собственности - она не обладает физическим признаком (не объективирована в конкретно осязаемой форме). В этом специфика машинной информации. Следовательно, ее нельзя похитить, повредить или уничтожить, как другое имущество. Единственно, она может выступать в качестве объекта авторского права, и в этом случае ответственность наступает по ст. 146 УК РФ (“Нарушение авторских и смежных прав”).

Следует согласиться с мнением профессора Комиссарова, что компьютерная информация не может рассматриваться в качестве предмета преступления. И не только потому, что виртуальная реальность отличается от реальной - как известно, в теории уголовного права под предметом понимается вещь материального мира. Значение предмета преступления в том, чтобы отграничивать одно преступление от другого. Так, например, кража (ст. 158 УК РФ) и хищение наркотических средств либо психотропных веществ (ст. 229 УК) или хищение предметов, имеющих особую ценность (ст. 164 УК), отграничиваются только по предмету преступления. И если виновное лицо совершило хищение наркотических средств из аптеки, то его действия будут квалифициро-

ваться по ст. 229 УК РФ, а если лекарства или денежные средства, то лицо будет привлечено у уголовной ответственности по ст. 158 УК.

С компьютерной информацией такую аналогию провести не получится. Если лицо осуществляет неправомерный доступ к компьютерной информации (ст. 272 УК), копирует ее и при этом данная информация составляет государственную тайну (ст. 275, 276 УК), то налицо не конкуренция норм, а совокупность преступлений. Если бы компьютерная информация была предметом, то она не могла бы фигурировать сразу в двух преступлениях. Также не может считаться предметом ст. 111 УК здоровье, а предметом ст. 105 УК жизнь, несмотря на то, что именно здоровью и жизни причиняется вред, как и компьютерной информации в преступлениях, предусмотренных ст. 272, 273, 274 УК РФ.

Введение законодателем в УК термина "компьютерная информация" является вполне обоснованным решением, цель которого - отграничение преступлений в сфере компьютерной информации от иных информационных преступлений, предусмотренных другими разделами УК. Поскольку компьютерная информация - это совокупность сведений экономического, политического, социального, правового характера, постольку очевидно, что в каждом случае совершения компьютерных преступлений всегда будет страдать какой-либо дополнительный объект - то общественное отношение, нормальное существование которого зависит от степени защищенности информации.

Таким образом, под компьютерной информацией следует понимать данные и программы, существующие в электронном виде, которые могут храниться на машинном носителе или использоваться в работе компьютерной техники и ее сети.

1. *Лопатина Т.М.* Виктимологическая профилактика компьютерных преступлений // Рос. юстиция. 2006. № 4. С. 92.

2. См.: *Згадзай О.Э., Казанцев С.Я., Казанцева Л.А.* Информатика для юристов: учебник / под. ред. С.Я. Казанцева. М., 2001. С. 218.

3. См.: *Наумов А.В.* Российское уголовное право: курс лекций. В 3 т. Т. 3. Особенная часть. 4-е изд., перераб. и доп. М., 2008

4. Уголовное право. Особенная часть: учебник / отв. ред. И.Я. Козаченко, Г.П. Новоселов. М., 2008.

5. Уголовное право. Особенная часть: учебник / под ред. А.И. Рарога. М., 2009.

6. *Стрельцов А.А.* Обеспечение информационной безопасности России: теоретические и методологические основы / под ред. В.А. Садовничего, В.П. Шерстюка. М., 2002.

7. *Юсупов Р.М., Заболотский В.П.* Научно-методологические основы информатизации. СПб., 2000.

8. Колобов В.А. Информационная безопасность и антитеррористическая деятельность современного государства: проблемы правового регулирования и варианты их решения / В.А. Колобов, В.Н. Ясенев. Н. Новгород, 2001. С. 37.

9. Комментарий к Уголовному кодексу Российской Федерации с постатейными материалами и судебной практикой / В.Б. Боровиков [и др.]; под общ. ред. С.И. Никулина. М., 2001.

10. *Максимов В.Ю.* Компьютерные преступления (вирусный аспект). Ставрополь, 1999.

11. *Волеводз А.Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., 2002.

12. *Смирнова Т.Г.* Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: дис. ... канд. юрид. наук. М., 1998.

13. *Батурин Ю.М., Жодзишский А.М.* Компьютерные правонарушения: криминализация, квалификация, раскрытие // Советское государство и право. 1990. № 12.

14. *Ахраменка Н.Ф.* Компьютерная безопасность как родовой объект информационных преступлений // Комплексная защита информации: тез. докл. VII Междунар. конф., Раубичи, 25 - 27 февр. 2003 г. / отв. ред. А.П. Леонов. Минск, 2003.

15. Преступления в сфере компьютерной информации: квалификация и доказывание: учеб. пособие / под ред. Ю.В. Гаврилина. М., 2003.

16. Комментарий к Уголовному кодексу Российской Федерации. С постатейными материалами и практическими разъяснениями / авт. ком. и сост. А.Б. Борисов. М., 2008.

Поступила в редакцию 06.01.2011 г.