

Ю.А. Фисун, Р.А. Белевский, Р.А. Фисун
**КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ: ПРОБЛЕМЫ
ФОРМИРОВАНИЯ И РАЗВИТИЯ ПРАВОВЫХ НОРМ,
РЕГУЛИРУЮЩИХ ПРАВООТНОШЕНИЯ
В ИНФОРМАЦИОННОЙ СФЕРЕ**

Особенностью российского уголовно-правового законодательства в сфере компьютерных преступлений является общий подход к ответственности за совершение компьютерных преступлений (КП), для понимания которого необходимо его сравнение с уголовно-правовым законодательством зарубежных стран. Анализ мировой практики совершения преступлений в сфере новых информационных технологий (НИТ) показывает, что в настоящее время намечена тенденция перехода от "любительского хакерства" к высокопрофессиональному искусству совершения КП. Так, в Германии издается специализированный журнал хакеров, в котором специалисты-криптоаналитики делятся своим опытом по преодолению систем защиты конфиденциальной информации в компьютерных сетях.

Принятый в 1999 году странами Европейского Союза закон о придании юридического статуса электронным цифровым подписям документов, прошедших по Internet, содержит правила защиты и ответственности, обеспечивающие восприятия и распознавания фальсификации электронных цифровых подписей во всех странах ЕС. Постоянное возрастание компьютерных преступлений обуславливает интерес пользователей к программно-аппаратным и организационным комплексам защиты информации.

В ходе анализа известных работ уточнены следующие основные виды компьютерных преступлений, характерных и для России:

- 1) компьютерное мошенничество;
 - 2) подделка компьютерной информации;
 - 3) повреждение данных или программ, обрабатываемых и хранящихся в компьютерных банках данных;
 - 4) компьютерный саботаж;
 - 5) несанкционированный доступ (НСД) к информации локальных, распределенных, в том числе глобальных информационно-вычислительных сетей (ИВС);
 - 6) несанкционированный перехват данных с помощью технических средств съема информации с ИВС за счет побочных электромагнитных излучений и наводок;
 - 7) несанкционированное использование защищенных компьютерных программ.
- В рамках этих групп КП выделяются отличия российского уголовно-правового законодательства.

Первое отличие заключается в принадлежности российского законодательства к континентальной системе права, которой свойственно отдавать предпочтение общим, так называемым юридико-техническим конструкциям, целью которых является обобщение множества возникающих правовых ситуаций. Англосаксонская правовая система ориентирована на судебный прецедент, на группу очень схожих в деталях правонарушений.

Второе отличие заключается в том, что несмотря на относительно невысокий (по сравнению с западным) уровень развития информационно-компьютерной инфраструктуры в российском обществе, в нем стремительно растет распространение КП. При этом в российском законодательстве выделяют две группы КП: 1) преступления, направленные на незаконное овладение, изъятие, уничтожение либо

повреждение ЭВТ и носителей информации как таковых, не имеющие своей целью совершение противоправных действий с информацией, содержащейся на электронных носителях (глава 21 Уголовного кодекса РФ (УК РФ)); 2) преступления, направленные на получение НСД к компьютерной информации (КИ) (глава 28 УК РФ).

Ряд авторов предлагают ввести еще одно понимание КП, не содержащихся в уголовно-правовом законодательстве России, под которыми понимаются преступления, где ЭВМ и другие средства НИТ используются преступниками как средство совершения корыстного преступления, их умысел направлен на овладение чужим имуществом путем внесения изменений в программы и базы данных. Известна серьезная дискуссия о правильности квалификации преступлений, совершенных с использованием ЭВМ. По совокупности статей Главы 28 и Главы 21 УК РФ, высказывается мнение, что понятие "мошенничество" к компьютерным преступлениям не применимо. Существует мнение, что включенная в УК РФ специальная глава 28 "Преступления в сфере компьютерной информации" не в полной мере решает проблему хищения информации при помощи ЭВМ. Это относится и к существующей статье о мошенничестве с использованием ЭВМ и НИТ. Очевидно, что "поскольку законодатель счел целесообразным выделить специальную главу в связи со спецификой объекта, следовательно, по логике закона, необходим специальный состав, предусматривающий хищение путем использования ЭВМ".

С учетом развития экономических отношений возникает проблема развития уголовно-правового законодательства, в том числе и в части главы 28 УК РФ и создания новых квалифицирующих признаков. При этом можно ввести в статью 159 УК РФ квалифицирующий признак - "мошенничество, совершенное с использованием средств ЭВМ". Однако необходимость такого изменения законодательства не является однозначной. Здесь возникают проблемы криминологического аспекта группы КП против собственности, которые сложно решить одними лишь методами совершенствования законодательной техники. Считается, что здесь будет достаточно квалифицировать совершаемые корыстные компьютерные преступления по совокупности статей глав 22 и 28, обращая внимание на криминологические, криминалистические и уголовно-процессуальные аспекты в связи со сложностью раскрытия и доказывания вины при совершении подобного рода преступлений. Кроме этого существуют и другие проблемы.

По мнению Е.Р. Россинской, при формировании новых отраслей экспертного знания существует проблема экспертиз КП, для которых не всегда пригодны существующие аналоги в других отраслях права. С КП связана и проблема экстрадиции лиц. В рамках формирования правовых норм, регулирующих отношения в информационной сфере, весьма актуальной и своевременной является задача развития тех норм, которые определяют юридическую ответственность за КП. Важное место среди рассмотренных проблем занимает вопрос содержания юридической ответственности в области КИ, как важной меры защиты интересов личности, общества и государства в информационной сфере.

В связи с глобальной компьютеризацией информационных процессов в органах государственной власти особое место занимает проблема правонарушений в отношении конфиденциальной информации ЭВМ и ИВС, в том числе обладающей высокой степенью секретности. Это требует: а) разработки специальных средств наблюдения и регистрации действий пользователя в системе; б) признания журналов регистрации действий пользователя и других документов, отражающих действия персонала, работающего с конфиденциальной информацией, как доказательства для судов и

следственных действий. Следует также обратить внимание на распространенность отдельных правонарушений и их адресность.

Весьма актуальным является вопрос охраны конституционных прав личности при использовании НИТ, связанных с защитой персональных данных.

Важно при организации защиты КИ учитывать особенности законодательства об ответственности: необходимость четкого выявления предмета противоправного действия; доказательность противоправного действия; адресность действия и возможность выявления конкретного правонарушителя; значимость правонарушения (размеры ущерба). Обеспечение безопасности КИ предполагает решение вопросов гражданской и уголовной ответственности за незаконное приобретение и использование КИ, доказывания особенностей этих противоправных действий, выявления, раскрытия, расследования и предупреждения фактов преступного манипулирования программным продуктом и т. д. Это требует: 1) развития законодательства, анализа следственной и судебной практики; 2) привлечения к уголовной ответственности за компьютерные преступления; 3) разработки методики доказывания и судебных исследований КП; 4) развития технико-криминалистических, тактических и методических приемов, методов, средств раскрытия и расследования КП; 5) развития ИВС, подготовки квалифицированных специалистов; 6) развития правовой поддержки процесса обеспечения информационной безопасности, использования технических способов и средств защиты КИ.

Таким образом, можно говорить, что разработка теоретических и прикладных правовых вопросов защиты КИ является одной из важных проблем развития правовой науки и неперенным условием комплексного обеспечения информационной безопасности информационной сферы. Следовательно и проблема развития законодательства в области борьбы с компьютерными преступлениями, выходит далеко за рамки одного лишь уголовно-правового законодательства и требует, в силу своей специфики, комплексного подхода к развитию правовых норм ряда отраслей права и других научных направлений.