С О Д Е Р Ж А Н И Е

**стр.**

# ВВЕДЕНИЕ . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2

1. Проблемы уголовно-правового регулирования

в сфере компьютерной информации . . . . . . . . . . . . . . . . . . . 3

1. Компьютерная безопасность,

мировой опыт, мировые проблемы . . . . . . . . . . . . . . . . . . . . 11

1. Доказательство в судебных делах

по компьютерным преступлениям . . . . . . . . . . . . . . . . . . . . . 15

ЗАКЛЮЧЕНИЕ . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 18

Список используемой литературы . . . . . . . . . . . . . . . . . . . . . . . . 19

### В В Е Д Е Н И Е

Компьютерные преступления приобрели в странах с развитой телекоммуникационной инфраструктурой настолько широкое распространение, что для борьбы с ними в уголовное законодательство были введены специальные составы преступлений. Традиционные меры гражданско-правовой ответственности, ориентированные, прежде всего на возмещение убытков, не смогли сыграть роль сдерживающего фактора и воспрепятствовать широкому распространению этого вида правонарушений.

Говоря о системе безопасности, необходимо иметь четкое представление о том, что она защищает и от чего (или от кого), поскольку главной функцией системы безопасности является противодействие угрозам со стороны людей и техники. Каждая реализованная угроза влечет за собой тот или иной ущерб. Противодействие реализации угрозы призвано снизить величину ущерба до минимума. Оценка вероятности появления угроз и ожидаемых размеров потерь является достаточно сложной задачей. В связи с этим при реализации политики безопасности и выборе системы защиты в первую очередь учитывают такие факторы, как бесконфликтность работы выбранных средств защиты, возможность получения полной информации о механизмах защиты и способах противодействия ей, а также гарантии, предоставляемые пользователям со стороны изготовителей.

1. Проблемы уголовно-правового регулирования в сфере компьютерной информации

Современный этап развития общества характеризуется бурным развитием и внедрением средств связи, вычислительной техники и новых информационных технологий практически во все сферы человеческой деятельности. Все это привело к формированию так называемого «кибернетического пространства», впитавшего в себя не только общечеловеческие культурные ценности, но, к сожалению, и все присущие обществу пороки.

Так, пользователь информационной сети может свободно получить рецепты производства наркотиков, способы изготовления из доступных материалов самодельных взрывных устройств, переписать на свой компьютер порнографические изображения или мультимедийные журналы «сомнительного содержания», получить полные тексты доктрин идейных руководителей нацизма и мирового терроризма, принять участие в электронной конференции хакеров, на которой обсуждаются вопросы несанкционированного проникновения в автоматизированные системы органов государственного управления, военных структур и т.п.

Назревшая необходимость в установлении ответственности за правонарушения, совершаемые в области компьютерных технологий, предопределила соответствующие законодательные инициативы. В частности, в Уголовный Кодекс Российской Федерации 1996 года внесены принципиально новые для отечественного уголовного законодательства виды преступлений, объединенные в самостоятельную 28-ю главу УК – «Преступления в сфере компьютерной информации». Такой подход, несомненно, верен и соответствует мировым правовым тенденциям.

Однако, давно известно, что написанный с использованием неоднозначно трактуемых категорий и понятий закон чреват существенными негативными последствиями в будущем при его практическом применении, особенно если этот закон уголовный.

Отсутствие в нашей стране опыта уголовно-правового регулирования «компьютерных правоотношений» в области такого достаточно пока необычного для многих (в том числе и для законодателей) объекта как «кибернетическое пространство» повлекло за собой то, что ряд формулировок уголовно-правовых новелл страдает отмеченным выше недостатком.

С криминалистической точки зрения, наиболее важным для правильной квалификации преступления в сфере компьютерной информации является факт представления этой информации в виде, предназначенном и пригодном для ее обработки, хранения и передачи с использованием электронных технических средств, список которых не ограничивается исключительно компьютерами. При этом смысловое содержание информации уходит на второй план, так как в машинном виде оно всегда представлено одинаково – в виде, определяемом физической природой материального носителя информации.

Для определения местонахождения компьютерной информации более правильным представляется использование введенного Законом Российской Федерации «Об информации, информатизации и защите информации» понятия «материальный носитель информации», в который наряду с машинными носителями входит и электромагнитный сигнал, использующийся при информационном обмене между ЭВМ по радиоканалу, электрическому или оптоволоконному кабелю и т.п.

Необходимость учета данного факта в уголовном законодательстве ряда промышленно развитых государств мира (например, в Канаде) привела к формированию двух относительно самостоятельных групп преступных деяний в сфере информатизации и новых информатизационных технологий: «компьютерных преступлений» и «коммуникационных преступлений». Отсутствие подобного деления в российском уголовном законодательстве, а также возникновение реальных уголовных дел, связанных с доступом к компьютерной информации через радиоканал, требует более тщательной правовой проработки этого вопроса.

Существует большое число информационных систем и сетей, не имеющих собственника, однако широко использующихся в серьезных практических приложениях. Ярким примером может служить всемирная сеть Internet.

Включение в определение компьютерной информации термина «идентифицируемый элемент информационной системы» является неоправданным. Идентификация компьютерной информации в рамках выявления и расследования преступлений в рассматриваемой сфере представляет собой самостоятельную и исключительно сложную криминалистическую задачу, которая в настоящее время не имеет однозначно положительного решения.

Более того, специфика компьютерной информации, ее способность к копированию (перемещению без изъятия из первоначального места расположения), отсутствие у нее ярко выраженных индивидуальных свойств приводит к необходимости проведения определенных криминалистических действий по преобразованию информации на материальном носителе в документированную информацию, то есть в такую «организационную форму, определяемую как совокупность:

а) содержания информации;

б) реквизитов, позволяющих установить источник, полноту информации, степень ее достоверности, принадлежность и другие параметры;

в) материального носителя информации, на котором ее содержание и реквизиты закреплены».

При этом идентификация компьютерной информации будет проводиться на основе документированной.

Таким образом, компьютерную информацию как объект преступного посягательства, правильнее было бы определить следующим образом:

*Компьютерная информация* – это информация, представленная в специальном (машинном) виде, предназначенном и пригодном для ее автоматизированной обработки, хранения и передачи, находящаяся на материальном носителе и имеющая собственника, установившего порядок ее создания (генерации), обработки, передачи и уничтожения.

Вторым базовым понятием, широко используемом в статьях Уголовного кодекса, посвященных преступлениям в сфере компьютерной информации является ЭВМ – электронная вычислительная машина. Большинство авторов комментариев УК для пояснения данного понятия используют классическое определение, заимствованное из технических наук, в соответствии с которым под ЭВМ понимается устройство, выполненное на электронных приборах и состоящее из ряда основных функциональных элементов: логических, запоминающих, индикационных и ряда других.

Приведенное определение ЭВМ является сложносоставным и для целей правового регулирования (и тем более уголовного) требует серьезной конкретизации. Отсутствие необходимой детализации в Уголовном кодексе неминуемо приведет к возникновению ряда вопросов, не имеющих однозначного юридического решения.

Большое значение для правильной квалификации преступлений в сфере компьютерной информации играет цель или мотив совершаемых деяний. Однако рассматриваемые статье УК, к сожалению, не содержат упоминаний о них, что приводит к серьезным трудностям в правоприменительной практике.

Как, например, следует расценивать научно-исследовательские работы (проводимые зачастую по инициативе и за счет государства) по изучению компьютерных вирусов (вредоносных программ) для выработки мероприятий по борьбе с ними, если такая деятельность фактически образуют состав преступления, предусмотренного ст. 273 УК Российской Федерации.

Уже несколько лет автор одного из наиболее популярных антивирусных программных продуктов Aidstest Д. Лозинский регулярно получает по электронной почте новые виды и модификации компьютерных вирусов для анализа. Таким образом, все, кто присылает ему эти вредоносные программы, делают благое дело, которое впоследствии позволит сотням и тысячам других людей избежать значительного ущерба от их воздействия. Однако если следовать букве закона, получается, что они совершают уголовное преступление, предусмотренное ст. 273 УК.

Весьма некорректной представляется формулировка части первой статьи 272 «Неправомерный доступ к охраняемой законом компьютерной информации…», т.к. проблематичным является выявление факта охраны компьютерной информации определенным законом.

По сложившейся практике, компьютерная информация в виде программ для ЭВМ, баз данных является объектом интеллектуальной собственности и охраняется законом после ее соответствующей регистрации. При этом подразумевается охрана авторских прав и всех вытекающих из этого правомочий. Однако в Уголовном кодексе существуют отдельные составы преступлений (ст. 147 «Нарушение избирательских и патентных прав» и ст. 180 «Незаконное использование товарного знака»).

Такой же некорректной представляется используемая в ст. 272 УК конструкция «нарушение работы ЭВМ». Данный термин заимствован из области техники и мало пригоден для построения юридических формулировок. Используя понятие ЭВМ как технического устройства, невозможно установить, что такое «работа ЭВМ», и оценить, нарушена она или нет.

Например, в результате неправомерного доступа к информации стерт один файл с программой обработки данных. В итоге ЭВМ работоспособна (то есть включается питание и проходят все необходимые тесты), на ней функционируют все вновь устанавливаемые программы, и лишь при запуске одной из них при выполнении определенной операции внутри этой программы ожидаемый результат не достигается. Следует ли такую ситуацию считать нарушением работы ЭВМ? Сформулированный вопрос обусловлен тем, что используемое техническое понятие «работа ЭВМ» не связано с конечным результатом вычислений, то есть с тем, ради чего ЭВМ используется.

Весьма расплывчата и формулировка части первой статьи 274 УК «Нарушение правил эксплуатации ЭВМ». Это связано в первую очередь с тем, что единых правил эксплуатации ЭВМ в настоящее время не существует, да и вряд ли таковые появятся в обозримом будущем, так как у различных компьютерных и построенных на их основе сетей существует слишком много технических особенностей.

Еще одним примером неудачного заимствования технического термина является применение конструкции «Создание программ для ЭВМ… заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации..."»(ст. 273 УК). В соответствии с классическим определением, программа для ЭВМ неразрывно связана с решаемой задачей. Таким образом, не указав, какая решается или должна решаться задача, нельзя установить, с чем мы имеем дело – с законченной программой или ее фрагментом. Например, при выполнении переноса (перемещения) программы с одного магнитного носителя на другой происходит последовательное выполнение двух действий – копирование и удаление (реализуемые соответствующими фрагментами программы перемещения), которые по отдельности могут рассматриваться как вполне законченные программы и, более того, упомянуты в ряде статей Уголовного кодекса.

Следует заметить, что при обработке информации любая программа заведомо создает, модифицирует и уничтожает данные. Поэтому представляется весьма затруднительным установить степень правомерности действий такого рода, особенно если учесть, что все они производятся за незначительный промежуток времени и в достаточно больших количествах.

Использование понятия «блокирование информации» в ряде статей УК РФ не соотнесено с назначением и важностью этой информации в той или иной технической или организационной системе и, как следствие, с масштабом времени, в котором она функционирует или управляется.

Уголовный закон, регулирующий отношения в сфере компьютерной информации, необходим. Но в настоящем виде он требует существенных уточнений и корректировок. Без этого невозможно представить себе адекватное его применение.

1. ***Компьютерная безопасность, мировой опыт,***

 ***мировые проблемы***

Минувший год был отмечен серьезным ростом сообщений о компьютерных преступлениях. Отчет Института компьютерной безопасности содержит следующие цифры: опрошено 563 организации, сумма прямых потерь в них составляет более 100 млн. долларов США, причем 75% опрошенных в качестве основных выделяют следующие опасности:

* кража финансовых данных и подделка финансовых документов сотрудниками;
* кража критичной информации уволенными сотрудниками;
* саботаж сотрудников, извещенных о предстоящем увольнении;
* кражи переносных компьютеров и их компонентов.

Ситуация сильно осложняется закрытостью статистической информации о совершенных и раскрытых преступлениях и правонарушениях.

Тема хищения баз данных, содержащих «деликатные» сведения, отнюдь не нова. Нетрудно предположить, какой простор деятельности открывает возможность манипулирования этой информацией представителям организованной преступности, различным махинаторам. Поэтому у многих первым делом возникает вопрос: каким образом становится возможной утечка столь важной информации?

Формирование подобных баз данных занимается достаточно большое количество государственных ведомств и ряд коммерческих структур. Основная сложность состоит в невозможности дать однозначный ответ на вопрос о происхождении данных. У всех баз, как правило, изменена оболочка, внесено что-то свое, тем самым информация лишена своих индивидуальных признаков и спрятаны концы, по которым можно было бы установить ее источник.

Есть еще одна проблема, с которой приходится сталкиваться следствию, - отсутствие заинтересованности со стороны пострадавших фирм к сотрудничеству с правоохранительными органами. Коммерческие структуры опасаются широкой огласки происшедшего из-за боязни потерять существующих и потенциальных клиентов. Подобная ситуация уже довольно давно стала характерной для кредитно-финансовой сферы на Западе, когда банку выгоднее смириться с незначительными потерями от тех или иных махинаций с электронной наличностью, чем позволить произойти оттоку части своей клиентуры, усомнившейся в его полной надежности.

С другой стороны, шила в мешке не утаишь, и потерпевшим все-таки стоит задуматься о том, что наведение порядка в собственном доме важно в первую очередь для них самих, поскольку в конечном итоге это только укрепит их позиции на рынке. А пока следствие вынуждено искать нетрадиционные пути решения этой проблемы, обращаясь к гражданам через телевидение с призывом заявлять о понесенном ими ущербе, поскольку формальные собственники похищенных баз данных этого делать не торопятся.

Важным аспектом проблемы распространения баз данных является то, что часть из них относится к разряду сведений, представляющих коммерческую тайну. Это позволяет следствию инкриминировать обвиняемым ст. 183, ч. 2 Уголовного Кодекса РФ, которая предусматривает ответственность «за незаконный сбор, разглашение и использование сведений, составляющих коммерческую тайну, без согласия владельца из корыстной или иной личной заинтересованности».

Статья 11 Закона РФ «Об информации, информатизации и защите информации» относит персональные данные к категории конфиденциальной информации и запрещает сбор, хранение, использование информации о частной жизни, а также информации, нарушающей личную тайну. Пункт 4 этой статьи однозначно указывает на то, что «подлежит обязательному лицензированию деятельность негосударственных организаций и частных лиц, связанная с обработкой и предоставлением пользователям персональных данных».

Если коммерческие структуры имеют лицензию на разработку и реализацию программного обеспечения, но фактически занимаются сбором и коммерческим распространением информационных баз, содержащих персональные данные – налицо признаки преступления, предусмотренного ст. 171, ч. 2 Уголовного Кодекса РФ, «нарушение условий лицензирования с причинением крупного ущерба и с извлечением дохода в особо крупных размерах».

Раскрытие компьютерных преступлений – нетрадиционная, нелегкая и порой дискуссионная проблема – как по причине сложности самого факта доказывания, так и в силу несовершенства действующего законодательства, которое позволяет обвиняемым «маневрировать» в оценке своего деяния.

Каковы же перспективы? Они достаточно туманны, и, прежде всего, потому, что наши силовые ведомства в этих случаях привыкли идти по накатанной схеме: оперативная разработка – задержание – арест – следствие – суд. В приведенной цепочке каждая служба решает свои собственные задачи, зачастую работа идет «от преступления» – есть сам факт, и надо найти преступника. В сфере компьютерных преступлений такая методика неприемлема. Компьютерный преступник высокоинтеллектуален, в традиционном понимании абсолютно законопослушен, зачастую одержим своими идеями. Поэтому для успешного противоборства с ними сотрудники МВД, ФСБ, прокуратуры, суды должны обладать соответствующими знаниями и подготовкой. Требуется создание специализированных подразделений, которые вели бы постоянный мониторинг компьютерных сетей, периодической специализированной печати и иных источников криминальной и околокриминальной информации, осуществляли ее быстрый анализ, оперативную поддержку и реализацию, возбуждение уголовного дела (естественно, при наличии состава преступления). Соединенные Штаты уже пошли по этому пути. В каждом отделении ФБР созданы специальные отделы по борьбе с компьютерными преступлениями, и все говорит за то, что было бы неплохо последовать их примеру.

1. ***Доказательство в судебных делах по компьютерным преступлениям***

Судебное расследование компьютерных преступлений обычно бывает более сложным, нежели других видов преступлений. Оно требует специальной технической подготовки и в большей степени зависит от показаний свидетелей-экспертов. Обвинение в процессе по делу о компьютерном преступлении должно строиться так, чтобы судья и присяжные, мало знающие о компьютерах и их работе, смогли разобраться в очень сложных технических документах. Свидетели должны убедительно объяснить, почему последствия «неосязаемой» потери данных, являющихся чьей-либо собственностью, или нарушение работы компьютера столь же серьезны, как и ущерб при хищении материальных ценностей (а часто и более серьезны).

Судебные дела по компьютерным преступлениям относительно новы для следователей и обвинителей. Лишь немногие судьи и присяжные имеют представление о компьютерных технологиях, поэтому отношение к компьютерным преступлениям с их стороны может значительно различаться. Одни считают такие преступления серьезными, другие, видя, что преступление не привело к хищению компьютеров или нанесению ущерба зданиям, могут недооценивать его последствия. В некоторых случаях слабое знание специфики проблемы судьей и присяжными может быть даже опасным, так как неверная интерпретация представленного доказательства иногда приводит к ошибочному заключению.

В качестве примера можно привести судебное разбирательство по известному делу Роберта Т. Мориса о внедрении программы-червя в сеть Internet в 1988 году. Эта программа не нанесла прямого материального ущерба, так как не были похищены или повреждены данные. Однако компьютерные центры потеряли миллионы за то время, которое ушло на выявление этой программы и когда не могла выполняться никакая другая работа, а также время, ушедшее на проверку и восстановление работоспособности систем. Во время судебного процесса обвиняемый подтвердил внедрение программы-червя, но заявил, что это было сделано без злого умысла, в результате чего он был осужден условно. И таких случаев, когда условное осуждение выбиралось в качестве наказания за компьютерные преступления, принесшие многомиллионный ущерб, немало.

Какие же основания позволяют утверждать, что факт совершения компьютерного преступления имел место? Что является его доказательством, уликой? В случае убийства ответ прост. Это отпечаток пальца на столе на месте преступления, след пули, записка, выпавшая из кармана убийцы, когда он убегал из комнаты. В случае мошенничества ответ более сложен. Например, если преступник вошел в компьютерную систему по чужому паролю и перевел деньги с одного счета на другой, будет ли контрольный журнал компьютера уликой преступления? Будет ли уликой распечатка этого контрольного журнала, сделанная на следующий день после совершения преступления? Или распечатки, сделанные в последующие дни? Или достаточно лишь копии этих распечаток? Типичный ответ юриста заключается в том, что все это может считаться доказательством при определенных обстоятельствах.

В судебных разбирательствах по компьютерным преступлениям часто возникает вопрос о том, какие файлы и другие компьютерные документы могут быть использованы в качестве доказательств правонарушения.

На сегодняшний день в разных законах (а тем более в законах разных стран) имеются существенные различия даже в определении того, что такое компьютеры и как они работают. Но все же рост компьютерных преступлений и судебных прецедентов по ним позволяет судам проявлять все большую осведомленность относительно того, какие доказательства и как должны представляться в ходе судебных разбирательств по компьютерным преступлениям, а правоохранительным органам разрабатывать процедуры проверки компьютерных доказательств во время расследования преступления и правила обращения с ними для представления в суд. Поскольку новый Уголовный кодекс России, где впервые появилась глава «Преступления в сфере компьютерной информации», вступил в силу только в январе 1997 года, в нашей стране пока не накоплен опыт судебных дел по компьютерным преступлениям и не разработаны документы, регламентирующие представление компьютерных доказательств.

### З А К Л Ю Ч Е Н И Е

История мирового технического прогресса знает немало примеров того, как новейшие достижения человеческой мысли, призванные служить во благо, использовались совсем не по назначению. Для поиска примеров не обязательно обращаться к эпохе великих открытий. Подтверждения этого факта, пусть не столь значительные и не всем заметные, можно обнаружить и в настоящем. Многие из них связаны с одной из характерных особенностей нашего времени – компьютерными технологиями.

Создать абсолютно стойкую систему защиты также невозможно, как невозможно создать универсальную систему взлома. Поэтому при использовании системы защиты необходимо четко представлять диапазон ее применимости и ее способность противостоять воздействию злоумышленников разной квалификации и оснащенности.

#### М.В. ЛАРИОНОВА

## Список используемой литературы

1. Закон Российской Федерации «Об информации, информатизации и защите информации» // Собрание Законодательства Российской Федерации. № 8. Ст. 609.
2. Комментарий Федерального Закона «Об информации, информатизации и защите информации». М.: Институт государства и права РАН, 1996.
3. Крылов В.В. Информационные преступления – новый криминалистический объект // Российская юстиция. 1997. № 4.
4. Крылов В.В. Информационные компьютерные преступления. М.: ИнфраМ-Норма, 1997.
5. Комментарий к УК Российской Федерации / Под ред. А.В. Наумова.
6. Защита информации. Конфидент. Информационно-методический журнал № 5, 1995.
7. Комментарий к УК Российской Федерации. Том 2. Особенная часть / Под ред. Ю. Скуратова и В. Лебедева.
8. Баев О.Я., Мещеряков В.А. «Проблемы уголовно-правового регулирования в сфере компьютерной информации».// «Защита информации. Конфидент», № 5, 1998.
9. Защита информации. Конфидент. Информационно-методический журнал № 6, 1997.
10. Горбатов В.С., Полянская О.Ю. «Доказательство в судебных делах по компьютерным преступлениям». // «Защита информации. Конфидент», № 6, 1997.
11. Защита информации. Конфидент. Информационно-методический журнал № 6, 1998.
12. Батурин Ю.М., Жодзишский А.М. «Компьютерная преступность и компьютерная безопасность». М.: Юридическая литература, 1991.
13. Никифоров И. «Компьютерные преступления». // «Защита информации. Конфидент», № 5, 1995.
14. Черешкин Д.С., Смолян Г.Л., Цыгичко В.Н. «Реалии информационной войны» // «Защита информации. Конфидент», № 4, 1996.
15. Завадский И.И. «Информационная война – что это такое?» // «Защита информации. Конфидент», № 5, 1996.
16. Защита информации. Конфидент. Информационно-методический журнал № 1, 1998.
17. Кузнецов П.А. «Информационная война и бизнес» // «Защита информации. Конфидент», № 6, 1996.
18. Рачук Т.В. «Уголовные наказания за информационные преступления» // «Защита информации. Конфидент», № 4, 1997.
19. Фоменков Г.В. «О безопасности в Internet» // «Защита информации. Конфидент», № 6, 1998.
20. Защита информации. Конфидент. Информационно-методический журнал № 3, 1998.
21. Защита информации. Конфидент. Информационно-методический журнал № 1, 1999.