Антон Серго
«Интернет и право»

(http://internet-law.ru/book)

«Бестселлер», 2003 - 272 с. ISBN 5-98158-002-X

ГЛАВА 10. КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ

Ловятся не самые опасные, а самые глупые.
Суровая действительность

Компьютерная сеть Интернет стремительно превратилась в общепланетарную информационную систему (для кого-то она глобальный справочник, для кого-то библиотека мировой культуры, для кого-то трибуна собственных суждений), она вобрала в себя не только достоинства глобальности, но и глобальные пороки. Возможности Сети все чаще становятся средством совершения противоправных деяний.

Усугубляется все это особенностями Сети, позволяющей наносить максимально возможный ущерб при минимуме затрат. Например, при хищениях: определив уязвимость компьютерной сети кредитно-финансового учреждения, для злоумышленника не принципиален размер кражи, поскольку в отличие от обычного ограбления у него нет необходимости бегать по улицам с «миллионом долларов мелкими купюрами». Зарубежный опыт[1] подтверждает сказанное. По данным ФБР США, среднестатистический ущерб от одного такого преступления составляет 650 тыс. долларов, а от обычного ограбления банка 9 тыс. долларов США.

Впрочем, еще до широкого распространения глобальных компьютерных сетей, в 1966 году компьютер был впервые[2] использован как инструмент для совершения кражи из Банка Миннесоты (США), а первый закон, посвященный компьютерным преступлениям, был принят в США (штат Флорида) только в 1978 году и предусматривал ответственность за модификацию, уничтожение, несанкционированный доступ компьютерных данных. Отечественный преступный первенец относится к концу 70-х, а надлежащая правовая база появилась лишь в середине 90-х.

Популяризация в Сети компьютерной преступности и деятельности хакеров[3] окружена неким ореолом безнаказанности и благородства. СМИ также подогревают интерес к этому виду деятельности, создавая атмосферу романтики и славы. Успешные вторжения хакеров в те или иные компьютерные объекты показывают уязвимость пользователей компьютерных сетей, которые, стремясь к упрощению обмена информации и ускорению ее обработки, теряют на безопасности.

---

[1] Отечественной статистикой по данному вопросу автор, увы, не располагает.

[2] Первый официально зарегистрированный в США случай использования компьютерной техники для совершения преступления.

[3] Автор использует этот термин в том виде, в котором он «раскручен» СМИ, прекрасно понимая, что означает он высокую квалификацию программиста, а не преступный характер его деятельности.

Американские правительственные и военные объекты уже давно являются излюбленным объектом внимания хакеров всех стран и де-факто стали «экзаменом» на статус профессионала. Считается, что одно из самых опасных вторжений в компьютерные системы министерства обороны США было совершено в далеком 1987 году. 17-летний хакер дошел до файлов системы управления ракетами США и базы ВВС «Robbins». Его присутствие обнаружили после того, как он снял копии программного обеспечения, оцениваемого в 1,2 млн. долларов, включая сверхсекретные программы искусственного интеллекта.

Талант хакера уже давно активно эксплуатируется, работая на третьих лиц для решения самых разных задач. Более того, хакеры привлекаются к сотрудничеству не только частными, но и государственными структурами. В этом направлении разведка работает не менее эффективно. Например, по имеющейся информации, в 1986–1989 годах немецкие хакеры по заданию КГБ СССР копировали секретные материалы из компьютерных сетей Пентагона и NASA. Аналогичное немецкие хакеры делали и для своей разведки. В 1990 году группа австралийских хакеров вывела из строя работу NASA на 24 часа.

Подобные случаи не уникальны. Американские компьютерные службы безопасности ежесуточно выдерживают тысячи атак; сколько из них оказываются успешными, никому не известно. Появляющаяся информация о вторжениях в системы управления ядерным оружием, космическими объектами, в системы жизнеобеспечения городов и отдельных учреждений (например, медицинских) заставляет с тревогой смотреть в завтрашний день.

За последние годы были взломаны: 1999 год — сайт Совета Безопасности России, 2000 — сайты Минприроды, Минюста, Совета Федерации, МГТС, УБЭП по г. Москве, 2001 — сайты Совет Федерации, Госкомстата, 2002 — сайты МВД, Правительства Москвы. Следует заметить, что сайт Госкомстата в течение 2001 года взламывался неоднократно, а «дыра» в системе защиты, через которую есть доступ к базе переписи населения остается открытой с октября 2002 года (несмотря на ее обсуждения на конференциях и семинарах, посвященных информационной безопасности)

Законодательство разных стран по-разному подходит к правовой оценке компьютерной преступности. Становится очевидным, что несогласованность законодательства, отсутствие четкого межгосударственного сотрудничества и неразвитость международного законодательства являются существенным тормозом в борьбе с такими явлениями.

Компьютерные преступления в российском законодательстве

Отечественное законодательство предусматривает уголовную ответственность за компьютерные преступления в главе 28 Уголовного кодекса, состоящей из трех статей:

Статья 272. Неправомерный доступ к компьютерной информации (Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети);

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ (Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами);

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред).

Нет необходимости подробно анализировать указанные статьи, поскольку их детальному анализу уже были посвящены многочисленные работы, а авторский «бестселлер» «Хакер и закон» в конце прошлого века около сотни раз[4] встречался автором на русскоязычных хакерских сайтах в России и за рубежом.

Разумеется, компьютерная сеть может быть не только объектом, но и средством преступления, в этом случае ответственность правонарушителя будет по совокупности преступлений. Как известно, с помощью компьютера можно совершить любое преступление, кроме изнасилования, поэтому количество применимых статей достаточно велико.

Не претендуя на исчерпывающий список противоправных деяний, которые могут быть совершены с использованием компьютера и/или сети, ниже

[4] Приятно отметить, что отечественные хакеры стремятся повышать свой уровень юридической грамотности, давая возможность друг другу ознакомиться с юридическими материалами о своей деятельности.

представлен перечень статей УК РФ, под действие которых они могут подпадать:

Статья 129. Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию).

Статья 130. Оскорбление (унижение чести и достоинства другого лица, выраженное в неприличной форме).

Статья 137. Нарушение неприкосновенности частной жизни (незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан).

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

Статья 146. Нарушение авторских и смежных прав.

Статья 147. Нарушение изобретательских и патентных прав (незаконное использование изобретения, полезной модели или промышленного образца, разглашение без согласия автора или заявителя сущности изобретения, полезной модели или промышленного образца до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству, если эти деяния причинили крупный ущерб).

Статья 158. Кража (тайное хищение чужого имущества).

Статья 159. Мошенничество (хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием).

Статья 163. Вымогательство (требование передачи чужого имущества или права на имущество или совершения других действий имущественного характера под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких).

Статья 165. Причинение имущественного ущерба путем обмана или злоупотребления доверием.

Статья 167. Умышленные уничтожение или повреждение имущества (если эти деяния повлекли причинение значительного ущерба).

Статья 168. Уничтожение или повреждение имущества по неосторожности (в крупном размере).

Статья 171. Незаконное предпринимательство (осуществление предпринимательской деятельности без регистрации или с нарушением правил регистрации, а равно представление в орган, осуществляющий государственную регистрацию юридических лиц, документов, содержащих заведомо ложные сведения, либо осуществление предпринимательской деятельности без специального разрешения (лицензии) в случаях, когда такое разрешение (лицензия) обязательно, или с нарушением условий лицензирования, если это деяние причинило крупный ущерб гражданам, организациям или государству либо сопряжено с извлечением дохода в крупном размере).

Статья 182. Заведомо ложная реклама (использование в рекламе заведомо ложной информации относительно товаров, работ или услуг, а также их изготовителей (исполнителей, продавцов), совершенное из корыстной заинтересованности и причинившее значительный ущерб).

Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну (собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений).

Статья 200. Обман потребителей (обмеривание, обвешивание, обсчет, введение в заблуждение относительно потребительских свойств или качества товара (услуги) или иной обман потребителей в организациях, осуществляющих реализацию товаров или оказывающих услуги населению, а равно гражданами, зарегистрированными в качестве индивидуальных предпринимателей в сфере торговли (услуг), если эти деяния совершены в значительном размере).

Статья 242. Незаконное распространение порнографических материалов или предметов (незаконные изготовление в целях распространения или рекламирования, распространение, рекламирование порнографических материалов или предметов, а равно незаконная торговля печатными изданиями, кино- или видеоматериалами, изображениями или иными предметами порнографического характера).

Статья 276. Шпионаж (передача, а равно собирание, похищение или хранение в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки иных сведений для использования их в ущерб внешней безопасности Российской Федерации, если эти деяния совершены иностранным гражданином или лицом без гражданства).

Статья 280. Публичные призывы к осуществлению экстремистской деятельности.

Статья 282. Возбуждение национальной, расовой или религиозной вражды (действия, направленные на возбуждение национальной, расовой или религиозной вражды, унижение национального достоинства, а равно пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, национальной или расовой принадлежности, если эти деяния совершены публично или с использованием средств массовой информации).

Статья 283. Разглашение государственной тайны (разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены).

Статья 354. Публичные призывы к развязыванию агрессивной войны.

Разумеется, этот перечень нельзя считать исчерпывающим. В то же время, рассмотрение различных направлений преступной деятельности в сфере высоких технологий показывает сильное отставание и несовершенство современного законодательства. Несмотря на это, компьютерные преступники регулярно привлекаются к уголовной ответственности.

Говоря о судебной практике в рассматриваемой сфере, стоит отметить ее несформированность и, вследствие этого, неоднородность. Приговоры, вынесенные различными судами по однотипным уголовным делам, зачастую расходятся в вопросах квалификации действий преступника и размеров наказания. Вот некоторые примеры[5].

19 января 1997 года Южно-сахалинским городским судом впервые в России был вынесен обвинительный приговор по статьям о компьютерных преступлениях. Студент Южно-сахалинского института экономики, права и информатики Г. за написание программы, подбиравшей пароли к адресам пользователей электронной почты, а также копирование информации из чужих почтовых ящиков получил два года лишения свободы условно и штраф в 200 минимальных размеров оплаты труда.

10 марта 1998 года следственным управлением ГУВД Свердловской области было возбуждено уголовное дело по признакам преступления, предусмотренного ч. I ст. 273 УК РФ по факту распространения вредоносных программ для ЭВМ. Именно так было квалифицировано следствием создание электронной доски объявлений, в одной из областей которой находилась подборка вирусов и «крэков» для программного обеспечения. Среди доказательств распространения вредоносных программ в обвинительном заключении были упомянуты и лог-файлы с данными о том, какой из пользователей доски объявлений получал доступ к подборке вирусов.

[5] Подборка по материалам П. Протасова (Программист. 2001, № 12 и 2002, № 2).

6 отделом УРОПД при ГУВД Санкт-Петербурга и области 2 сентября 1998 г. было возбуждено уголовное дело по признакам преступления, предусмотренного ст. 273 УК РФ по факту распространения компакт-дисков с программами, предназначенными для снятия защиты с программных продуктов, а также «взломанных» версий программ. «Крэки» в данном случае были признаны следствием вредоносными программами (следует заметить, что такая квалификация, хотя и правильна формально, но все-таки вызывает многочисленные споры). Также обвинение было в ходе следствия дополнено статьей 146 УК РФ («Нарушение авторских и смежных прав»).

Тагилстроевский районный суд города Нижнего Тагила Свердловской области рассмотрел уголовное дело по обвинению Р. по ст. 159, 183, 272, 273 УК РФ. В октябре-ноябре 1998 года Р., пользуясь своим служебным положением, совершил изменение ведомости начисления заработной платы на предприятии так, что у работников, которым начислялось более ста рублей, списывалось по одному рублю, эти средства поступали на счет, откуда их впоследствии снял Р. Изменения в программе были квалифицированы по статье 273, сбор сведений о счетах лиц, данные о которых были внесены в базу предприятия, — по статье 183, модификация этих данных — по статье 272, а получение начисленных денежных средств — по статье 159 УК РФ. Р. был приговорен к 5 годам лишения свободы условно с лишением права заниматься профессиональной деятельностью программиста и оператора ЭВМ сроком на 2 года.

6 февраля 1999 года было возбуждено уголовное дело по признакам преступления, предусмотренного ст. 272 УК. В ходе предварительного следствия было установлено, что с целью хищения чужого имущества обвиняемые Ч. и З. вступили в сговор, по которому Ч., работающий в фирме «Самогон», имея доступ к компьютерам фирмы, ввел в базу клиентов фирмы сфальсифицированную запись с реквизитами, назвав которые впоследствии, З. получил со склада фирмы продукцию стоимостью более 70 тысяч рублей. Действия Ч. квалифицированы на предварительном следствии по статье 272 УК РФ. Приговором Вологодского городского суда З. был осужден по статье 159 УК РФ («Мошенничество») к 5 годам, а Ч. по статьям 159 и 272 УК РФ к 6 годам лишения свободы условно.

12 марта 1999 года в Управлении РОПД при ГУВД Ростовской области было возбуждено уголовное дело по признакам ст. 272 УК. В ходе следствия по статье 272 было квалифицировано завладение компьютером и считывание с него информации, признанной следствием коммерческой тайной. Доступ к компьютеру производился в нарушение правил исполнительного производства, в ходе которого одному из обвиняемых ЭВМ была передана на хранение.

Следователем следственной части СУ при МВД Республики Башкортостан 23 июня 1999 г. было возбуждено уголовное дело по признакам преступления, предусмотренного статьей 158 УК РФ по факту несанкционирован-

ного доступа к сети Интернет. В ходе следствия обвинение было предъявлено М. и Н., их действия были переквалифицированы по статьям 183 («Незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну») и 272 УК РФ. В отличие от рассмотренных ранее дел, связанных с распространением программ, предназначенных для хищения паролей для доступа к сети Интернет и пользование впоследствии таким доступом за чужой счет, в данном случае статья 273 за это вменена не была. Хищение имен и паролей для доступа было квалифицировано по статье 183 УК. Статья 165 вменена не была, что представляется упущением следствия.

30 сентября 1999 года следователем следственного отделения РУ ФСБ России по Архангельской области было возбуждено уголовное дело по факту создания и распространения вредоносных программ: распространение «троянцев» было квалифицировано по статье 273 УК РФ, доступ к чужим паролям — по статье 272. Один из обвиняемых по делу получил 2 года лишения свободы условно, второй — 3 года реально, впрочем, он был освобожден из-под стражи в зале суда по амнистии.

8 октября 1999 года было возбуждено уголовное дело по признакам преступления, предусмотренного статьей 272 УК РФ, по факту несанкционированной модификации программы публичного поискового сервера НовГУ. В результате данного изменения на поисковой странице сервера появилась ссылка на страницу, содержащую порнографические изображения. В совершении данного преступления в ходе предварительного следствия обвинялся Ф. Впоследствии он был обвинен также в незаконном распространении и рекламировании порнографических материалов по статье 242 УК РФ («Незаконное распространение порнографических материалов или предметов»). По имеющейся информации, по делу был вынесен оправдательный приговор.

Нижегородский районный суд 6 марта 2000 года вынес приговор за аналогичное преступление по статьям 272 и 165 УК РФ в отношении четырех жителей Нижнего Новгорода, действовавших по той же схеме — получавших доступ к Интернету за счет других абонентов. Один из соучастников получил 3 года 1 месяц, трое других — по 2 года 1 месяц лишения свободы условно.

18 апреля 2000 года Шадринским городским судом был осужден к штрафу в 3000 рублей П., по статьям 272 и 165 («Причинение имущественного ущерба путем обмана или злоупотребления доверием») УК РФ. П. совершил весьма распространенное преступление — получал доступ к сети Интернет за чужой счет, пользуясь чужим именем и паролем. Имя и пароль он получил, прислав программу-«троянца» на компьютер-«жертву». В рассматриваемом нами примере суд квалифицировал несанкционированный доступ к чужому компьютеру с целью кражи пароля по статье 272, а пользование услугой доступа к Интернет — по статье 165 УК РФ. В данном случае обращает на себя внимание тот факт, что «троянскую» программу П., согласно его же собственным показаниям, послал на компьютер с предназначенной специально для

этого страницы на сервере в Интернет, адреса которой он «не помнит». (Можно предположить, что, говоря про такую страницу, П. просто избежал обвинения еще и по статье 273 УК РФ в распространении вредоносных программ.)

Сходное по квалификации дело было рассмотрено 9 февраля 2001 года Красногвардейским судом города Санкт-Петербурга. Программист М. был признан виновным по статье 273 УК РФ в 12 эпизодах распространения вредоносных программ и по статье 165 — в причинении имущественного ущерба путем обмана или злоупотребления доверием. С ноября 1998 по апрель 1999 года он рассылал клиентам пяти петербуржских интернет-провайдеров троянские программы, и получал логины с паролями, которыми пользовался для доступа в Интернет. Суд приговорил его к трем годам лишения свободы и штрафу в размере 300 минимальных размеров оплаты труда. Впрочем, лишаться свободы М. не пришлось — из-за амнистии.

Подводя итог краткому обзору, следует признать, что «компьютерные» статьи УК РФ благополучно «работают» и по ним регулярно привлекаются к ответственности компьютерные мошенники и хулиганы. Последнее время по ст. 272 и ст. 273 правоохранительными органами фиксируются сотни преступлений ежегодно.

В тоже время, иногда эти статьи используются не совсем по назначению. В следующих примерах речь пойдет о достаточно спорных делах: представляется, что квалифицированы действия обвиняемых по ним были не совсем правильно. В подобного рода делах несформированность практики применения статей УК РФ о компьютерных преступлениях становится особенно заметной.

9 ноября 1998 года УРОПД ГУВД Московской области было возбуждено уголовное дело по факту совершения неправомерного доступа к охраняемой законом компьютерной информации в кассовых аппаратах одного из частных предпринимателей города Павловский Посад. По статье 272 УК РФ в ходе следствия было квалифицировано изменение информации в контрольно-кассовых аппаратах, при которых записанная в них сумма выручки за смену искусственно занижалась. Контрольно-кассовые аппараты были признаны следствием разновидностью электронно-вычислительной машины.

1 сентября 1999 года следственной частью следственного управления при УВД Южного административного округа г. Москвы было возбуждено уголовное дело по признакам преступления, предусмотренного статьей 272 УК РФ, по обвинению П. В ходе следствия обвинение было дополнено статьями 273, 165, 327 (Подделка, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков), 183. По статье 272 было квалифицировано пользование телефоном-«двойником», позволяющим производить бесплатные звонки за чужой счет. В рассматриваемом примере сотовый телефон был признан следствием разновидностью ЭВМ, а написание программы, с помощью которой обычный телефон превращался в «двойник»,

— по статье 273. Информация о серийном и абонентском номерах телефона была признана органами следствия коммерческой тайной, что и обусловило появление в обвинении статьи 183.

Особенно часто попытки вменять статьи о компьютерных преступлениях в случаях, когда совершаются совершенно, казалось бы, не относящиеся к компьютерам действия, предпринимаются в случаях мошенничества с сотовыми телефонами. Так, органами предварительного следствия (Ленинский РОВД г. Ставрополя) статья 272 была вменена обвиняемому, пользовавшемуся доработанным сотовым телефоном-«сканером», который позволял производить звонки за чужой счет.

Случай не единичный: еще в 1998 году в Воронеже следователем УРОПД Воронежского УВД по сходному делу, но уже за изготовление подобных телефонов, обвиняемым на предварительном следствии также была вменена статья 272 УК РФ.

Как показывает анализ сложившейся к настоящему моменту правоприменительной практики по уголовным делам о преступлениях, предусмотренных главой 28 УК РФ, большая часть случаев применения статей этой главы приходится на преступления, в которых доступ к охраняемой законом компьютерной информации осуществляется в ходе приготовления к другому преступлению (обычно — к преступлению против собственности) или покушения на него. Очень часто в тех случаях, когда уголовное дело возбуждается по статье из 28 главы, в процессе расследования совершение преступлений против собственности вменяется дополнительно, после того, как следствием получена информация о том, что же было действительной целью действий преступника.

Ранее подобные действия органами следствия квалифицировались по статье 272 как получение несанкционированного доступа к охраняемой законом компьютерной информации, однако впоследствии от такого подхода пришлось отказаться, т.к. признаков данного преступления в действиях лиц, привлекаемых к ответственности не содержалось: в общем случае информация, имеющаяся в Интернете, находится в свободном доступе. Со временем следственные органы нашли иной путь: пользование услугой за чужой счет квалифицируется по статье 165 УК РФ как причинение имущественного ущерба путем обмана. В случае, если украденные «логин» и «пароль» содержались в компьютере, откуда были похищены, дополнительно может быть вменена статья 272 УК РФ.

При использовании преступником сети Интернет очень часто возникают ситуации, когда компьютер, на котором находится информация, являющаяся объектом неправомерного доступа, либо, наоборот, получающий доступ к компьютеру преступник, расположен за пределами Российской Федерации. Общее правило, принятое в большинстве государств, требует применения закона той страны, в которой находится лицо, совершившее престу-

пление. Поэтому лица, находящиеся в России, несут ответственность за совершенное преступление по Уголовному кодексу РФ. Соответственно, в случае неправомерного доступа россиянина к информации, находящейся в ЭВМ, расположенной за пределами страны, следует применять отечественное уголовное законодательство, что прямо закреплено в статье 11 УК РФ.

Достаточно показательным судебным процессом, иллюстрирующим те трудности, которые возникают в подобных ситуациях, может служить дело по обвинению российских граждан И. и Г., которые осуществляли несанкционированный доступ к компьютерным сетям компаний, занимающихся электронной коммерцией, похищали оттуда номера кредитных карт клиентов, а затем шантажировали эти компании, предлагая за плату скрыть информацию, которая способна скомпрометировать компанию: не распространять номера карт и не оглашать сам факт неправомерного доступа.

Агенты ФБР в ходе расследования выманили И. и Г. на территорию США, предложив им работу в специально созданной фиктивной компании. Им было предложено протестировать компьютерную систему компании, при этом сотрудники ФБР воспользовались программами, зафиксировавшими все, что И. с Г. набирали на клавиатуре. В итоге ФБР получило пароли к компьютерам преступников, а при помощи паролей — доступ к самим компьютерам, с дисков которых была скачана информация, использованная впоследствии в качестве доказательства в суде.

8 августа 2002 года Челябинское отделение ФСБ возбудило уголовное дело по признакам преступления, предусмотренного частью 1 статьи 272 УК РФ. В официальном пресс-релизе УФСБ Челябинской области говорится, что дело было возбуждено по факту неправомерного доступа к охраняемой законом информации, находившейся на сервере частного предприятия, принадлежащего Г.

Также при расследовании было установлено, что неправомерно скопированная с компьютера Г. информация содержала в том числе и коммерческую тайну, охраняемую статьей 132 Гражданского кодекса РФ. При проведении экспертизы системного блока компьютера частного предприятия сотрудниками НИИИТ ФСБ России было установлено, что доступ к нему осуществлялся с территории США в период с 15 по 22 ноября 2000 года. Хотя прямо в официальных документах этого и не говорилось, но в преступлении подозревались сотрудники ФБР США, которые сам факт доступа, собственно, и не скрывали.

Ранее, судом США, по данному делу в мае 2001 года уже было вынесено судебное решение о признании доказательств, добытых при доступе к компьютерам Г. и И., полученными правомерно. Суд основывал его на том, что для обыска компьютера, находящегося вне Соединенных Штатов, ордер получать не нужно, а также на том, что задержка в получении улик могла привести к их уничтожению (практика производства следственных действий

без получения на то санкции суда в случаях, не терпящих отлагательства, принята и в отечественном УПК).

В связи с этим основное требование статьи 12 УК РФ («признание действий лица преступлением в той стране, на территории которой оно их совершило») соблюдено не было. При таких условиях возбуждение уголовного дела сотрудниками ФСБ выглядит скорее как шаг политический, а не процессуальный. Не совсем понятно также и то, почему ФСБ возбудило уголовное дело по статье, отнесенной статьей 151 УПК РФ к подследственности следователей ОВД, и проводило по нему предварительное следствие.

Тем не менее, возникшие тенденции в отечественной практике расследования и судебного рассмотрения уголовных дел о компьютерных преступлениях, позволяют надеяться на то, что спорные вопросы в их квалификации со временем получат разрешение и трудностей станет меньше, чем в настоящий момент».

Итак, появление в Уголовном Кодексе РФ 1996 года главы 28 («Преступления в сфере компьютерной информации») было очень своевременным. Волна компьютерной преступности уже пошла, а надлежащей правовой базы еще не было. С позиций сегодняшнего дня можно уже спорить о неудачности отдельных формулировок статей этого раздела, об узости охвата, о мягкости наказания и так далее. Тем не менее, правовые механизмы привлечения к ответственности за компьютерные преступления есть и они работают. В то же время зарубежное законодательство в этой сфере более развито и было бы неплохо перенять лучшее из зарубежного опыта.

Компьютерные преступления в зарубежном законодательстве

Законодательство разных стран по-разному подходит к проблематике компьютерных преступлений. На это влияет множество факторов: национальная правовая система, история развития, современное экономическое положение и многое-многое другое.

Не ставя целью полностью охватить все зарубежное законодательство, посвященное компьютерным преступлениям, в настоящем разделе собраны тезисные указания на компьютерные деяния, предусматривающие уголовную ответственность по законодательству разных стран[6].

США:

- компьютерный шпионаж,
- несанкционированный доступ к информации из компьютера используемого правительственным ведомством,
- повреждение или нарушение функционирования компьютера используемого правительственным ведомством,
- мошенничество с использованием компьютера,
- мошенничество путем торговли компьютерными паролями или аналогичной информацией при определенных обстоятельствах,
- угрозы, вымогательство, шантаж и другие противоправные деяния, совершаемые с помощью компьютера,
- торговля похищенными или поддельными устройствами доступа, которые могут быть использованы для получения денег, товаров или услуг,
- умышленное повреждение имущества, оборудования, линий и систем связи,
- перехват и разглашение сообщений, передаваемых по телеграфу, устно или электронным способом,
- нарушение конфиденциальности электронной почты и голосовых сообщений,

[6] Подборка подготовлена на основе: Волеводз А. Г. Противодействие компьютерным преступлениям. М., 2002 г.

- умышленное получение или видоизменение сообщений, хранящихся в памяти компьютера, а также за создание препятствий для санкционированного доступа к таким сообщениям.

Великобритания:

- умышленный противозаконный доступ к компьютеру или содержащейся в нем компьютерной информации или программам,
- неправомерный доступ к компьютерной информации на машинном носителе, в компьютере, компьютерной системе или сети, с целью или если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы компьютера, компьютерной системы или сети,
- разглашение персональных данных (в т. ч. с использованием компьютерной техники),
- изготовление и распространение порнографических материалов с использованием компьютерной техники.

Канада:

- несанкционированное получение любых компьютерных данных и услуг,
- несанкционированный перехват, прерывание, отслеживание, запись с использованием каких-либо устройств любых компьютерных данных,
- использование или принуждение к использованию компьютерных систем для совершения преступлений против собственности,
- умышленное несанкционированное изменение или уничтожение компьютерных данных,
- умышленное распространение бессмысленных, бесполезных или безрезультатных компьютерных данных и программ,
- умышленное создание затруднений, помех для законного использования общедоступных компьютерных данных,
- использование компьютерных технологий в целях извлечения прибыли путем создания финансовых «пирамид» и аналогичных махинаций.

Германия:

- неправомерный доступ к компьютерной информации,
- несанкционированная модификация компьютерной информации или ее использование,
- несанкционированное изменение, модификация, подделка или утаивание электронных данных,

- разрушение, повреждение, приведение в негодность технических средств обработки информации,
- нарушение тайны телекоммуникационной связи,
- компьютерное мошенничество,
- незаконное вмешательство в работу телекоммуникационных систем.

Франция:

- перехват, хищение, использование или предание огласке сообщений, передаваемых средствами связи,
- незаконный доступ к автоматизированной системе обработки данных,
- нарушение или воспрепятствование нормальной работе компьютерной системы,
- уничтожение или модификация информации в автоматизированной информационной системе,
- ввод или хранение в памяти ЭВМ запрещенных законом данных,
- нарушение порядка автоматизированной обработки персональных данных,
- сбор и обработка данных незаконным способом,
- хранение определенных данных сверх установленного законом срока,
- несанкционированное использование данных,
- уничтожение, порча или хищение любого документа, техники, сооружения, оборудования, установки, аппарата, технического устройства или системы автоматизированной обработки данных или внесение в них изменений,
- изготовление и распространение по телекоммуникационным сетям детской порнографии,
- сбор или передача содержащейся в памяти ЭВМ или картотеке информации иностранному государству, уничтожение, хищение, изъятие или копирование данных, носящих характер секретов национальной обороны, содержащихся в памяти ЭВМ или в картотеках, а также ознакомление с этими данными посторонних лиц,
- террористические акты, связанные с деяниями в области информатики.

Швеция:

- нарушение почтовой и телекоммуникационной тайны,

- незаконное получение доступа к информации в системах автоматической обработки данных или незаконное изменение, стирание или добавление в них данных,
- мошенничество путем предоставления неправильной или неполной информации, или внесения изменений в программу или отчетность, или какими-либо другими способами влияние на результат автоматической обработки информации или любой другой сходной автоматической обработки, которая влечет выгоду для лица, совершившего преступление, и убытки для любого другого лица,
- изготовление, сбыт и распространение детской порнографии.

Нидерланды:

- неправомерное вторжение в компьютер, компьютерную систему или компьютерную сеть, если вследствие этого нарушаются правила безопасности либо такой доступ осуществляется с помощью технических средств, ложных сигналов, ключей, полномочий;
- неправомерное проникновение в компьютер, компьютерную систему или сеть с копированием данных,
- неправомерное проникновение в компьютер, компьютерную систему или сеть с использованием телекоммуникационных устройств, если это совершается с целью извлечения незаконных доходов или для доступа в компьютер или компьютерную систему третьих лиц,
- несанкционированные перехват и запись с использованием технических устройств данных, передаваемых с использованием компьютерных устройств или общедоступных компьютерных сетей,
- установка технических устройств, предназначенных для перехвата и записи сообщений,
- умышленное уничтожение, изменение, блокирование информации, хранящейся в компьютере, компьютерной системе или сети,
- умышленное разрушение, повреждение или приведение в негодность компьютерного устройства или системы для хранения или обработки данных или любого телекоммуникационного устройства, а равно нарушение работы такого устройства,
- разглашение с корыстной целью данных, составляющих коммерческую тайну, полученных в результате несанкционированного вторжения в компьютерные устройства или системы,
- умышленное незаконное разрушение, уничтожение или иным способом приведение в негодность компьютерного устройства или системы для хранения и обработки данных или телекоммуникационных устройств,

- незаконный перехват, запись и разглашение данных, передаваемых по сетям телекоммуникации, с использованием служебного положения, а равно предоставление возможностей для этого третьим лицам,
- изготовление и использование с целью получения дохода подложных карт, предназначенных для компьютеризированных денежных сделок,
- распространение детской порнографии с использованием компьютерных технологий,
- шантаж, вымогательство с угрозой уничтожения данных, сохраняемых в компьютере или компьютерной системе,
- уклонение от оплаты услуг в сфере телекоммуникаций,
- взятка за содействие незаконному перехвату или записи телекоммуникационных сообщений.

Дания:

- незаконный доступ к информации или программам, предназначенным для использования в связи с электронной обработкой данных,
- дополнение, уничтожение, модификация информации или компьютерных программ в корыстных целях извлечения незаконной прибыли,
- незаконный доступ и использование информации, составляющей коммерческую тайну,
- незаконное использование информации, касающейся частной жизни человека,
- распространение детской порнографии.

Швейцария:

- неправомерное приобретение данных,
- неправомерное проникновение в систему переработки данных,
- повреждение данных,
- мошенничество с системами обработки данных,
- производство и распространение систем, предназначенных для незаконной расшифровки кодированной информации,
- незаконное получение доступа к персональным данным,
- нарушение почтовой и телекоммуникационной тайны.

Испания:

- раскрытие и распространение сообщений электронной почты, сведений хранящихся в электронных базах данных,

- использование телекоммуникаций без согласия собственника, повлекшее причинение ущерба,
- серийное производство или владение средствами, предназначенными для нейтрализации средств защиты программ для ЭВМ,
- завладение или раскрытие коммерческой тайны с использованием электронных документов или информационных устройств,
- изготовление или владение компьютерными программами или аппаратами, специально предназначенными для совершения преступлений,
- перехват телекоммуникационных сообщений с использованием должностного положения,
- передача по телекоммуникационным сетям ложных сообщений или фальсификация сообщений с использованием должностного положения,
- шпионаж, связанный с модификацией или раскрытием информации,
- раскрытие и выдача тайны и информации, связанных с национальной обороной.

Представленный перечень, разумеется, не является исчерпывающим, однако дает четкое представление об основных деяниях, признаваемых преступлениями в зарубежных странах. Указанная информация является весьма полезной в дискуссиях об изменениях главы 28 УК РФ.

Международное законодательство

Стремительное развитие трансграничной компьютерной преступности поставило мировое сообщество перед необходимостью налаживания международного сотрудничества и совместного противодействия компьютерным преступникам. Все это потребовало оперативной разработки надлежащей правовой базы. В итоге был принят ряд документов. В числе наиболее интересных и близких — опыт Европы и СНГ.

Первым документом Совета Европы, посвященным компьютерной преступности, была Рекомендация № R 89 (9) Комитета Министров стран-членов Совета Европы о преступлениях, связанных с компьютерами, принятая 13 сентября 1989 г. В ней определены практически все преступления, связанные с использованием компьютерных технологий, а также дана глубокая классификация компьютерных преступлений с рекомендуемым и факультативным перечнем включения их в национальное законодательство.

К перечню правонарушений, рекомендованных к включению в национальное законодательство, отнесены:

1. Компьютерное мошенничество (введение, изменение, стирание или подавление компьютерных данных или компьютерных программ или иное вмешательство в процесс обработки данных, которое влияет на результат обработки данных, что причиняет экономический ущерб или приводит к утрате собственности другого лица, с намерением получить незаконным путем экономическую выгоду для себя или для другого лица).

2. Компьютерный подлог (введение, изменение, стирание или подавление компьютерных данных или компьютерных программ или иное вмешательство в процесс обработки данных, совершаемое таким способом или при таких условиях, как это устанавливается национальным законодательством, при которых эти деяния квалифицировались бы как подлог, совершенный в отношении традиционного объекта такого правонарушения).

3. Причинение ущерба компьютерным данным или компьютерным программам (противоправное стирание, причинение ущерба, ухудшение качества или подавление компьютерных данных или компьютерных программ).

4. Компьютерный саботаж (введение, изменение, стирание или подавление компьютерных данных или компьютерных программ или создание помех компьютерным системам с намерением воспрепятствовать работе компьютера или телекоммуникационной системы).

5. Несанкционированный доступ (неправомочный доступ к компьютерной системе или сети путем нарушения охранных мер).

6. Несанкционированный перехват (неправомерный и осуществленный с помощью технических средств перехват сообщений, приходящих в компью-

терную систему или сеть, исходящих из компьютерной системы или сети и передаваемых в рамках компьютерной системы или сети).

7. Несанкционированное воспроизведение охраняемой авторским правом компьютерной программы (неправомерное воспроизведение, распространение или передача в общественное пользование компьютерной программы, охраняемой законом).

8. Несанкционированное воспроизведение микросхемы (неправомерное воспроизведение охраняемой законом микросхемы изделия на полупроводниках или неправомерное коммерческое использование или импорт с этой целью микросхемы или изделия на полупроводниках, изготовленного с использованием этой микросхемы).

К факультативному перечню были отнесены:

1. Неправомерное изменение компьютерных данных или компьютерных программ.

2. Компьютерный шпионаж (приобретение недозволенными методами или раскрытие, передача или использование торговой или коммерческой тайны, не имея на то права или любого другого правового обоснования, с целью причинить экономический ущерб лицу, имеющему доступ к этой тайне, или получить незаконную экономическую выгоду для себя или для третьего лица).

3. Несанкционированное использование компьютера — неправомерное использование компьютерной системы или сети, которое совершается:

- с пониманием того, что лицо, имеющее право на использование системы, подвергает ее значительному риску ущерба или системе или ее функционированию причиняется ущерб, или
- с намерением причинить ущерб лицу, имеющему право на использование системы, или системе или ее функционированию, или
- причиняет ущерб лицу, имеющему право на использование системы, или системе или ее функционированию.

4. Несанкционированное использование охраняемой законом компьютерной программы (неправомерное использование компьютерной программы, которая охраняется законом и которая воспроизводится без права на воспроизведение, с намерением обеспечить незаконную экономическую прибыль для себя или для другого лица или причинить ущерб обладателю соответствующего права).

Другим важным документом в рассматриваемой сфере является международная «Конвенция о киберпреступности».

Конвенция содержит указание на основные виды компьютерных правонарушений и меры, которые в связи с этим следует принять на национальном уровне.

К числу основных правонарушений Конвенция относит:

1. Преступления против конфиденциальности, целостности и доступности компьютерных данных[7] **и систем**:

- противозаконный доступ (доступ, когда он является преднамеренным, к компьютерной системе в целом или любой ее части без права на это, если он совершен с нарушениями мер безопасности и с намерением завладеть компьютерными данными или иным злым умыслом, или в отношении компьютерной системы, соединенной с другой компьютерной системой).
- противозаконный перехват (преднамеренно осуществленный с использованием технических средств перехват без права на это не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные, если совершено со злым умыслом или в отношении компьютерной системы, соединенной с другой компьютерной системой).
- воздействие на данные (преднамеренное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных без права на это).
- воздействие на функционирование системы (преднамеренное создание серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных).
- противозаконное использование устройств (производство, продажа, владение, приобретение для использования, импорт, оптовая продажа или иные формы предоставления в пользование: устройств, компьютерных программ, разработанных или адаптированных для целей совершения правонарушений; компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части с намерением использовать их с целью совершения правонарушения.

2. Правонарушения, связанные с использованием компьютерных средств:

- подлог с использованием компьютерных технологий (ввод, изменение, стирание или блокирование компьютерных данных влекущих за собой нарушение аутентичности данных с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, незави-

[7] «Компьютерные данные» означают любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные заставить компьютерную систему выполнять ту или иную функцию.

симо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными).

- мошенничество с использованием компьютерных технологий (преднамеренное и несанкционированное лишение другого лица его собственности путем любого ввода, изменения, удаления или блокирования компьютерных данных либо любого вмешательства в функционирование компьютерной системы, с мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица).

3. **Правонарушения, связанные с содержанием данных — детская порнография** (преднамеренное и несанкционированное производство детской порнографической[8] продукции с целью распространения через компьютерную систему; предложение или предоставление в пользование детской порнографии через компьютерную систему; распространение или передача детской порнографии через компьютерную систему; приобретение детской порнографии через компьютерную систему для себя или для другого лица; владение детской порнографией, находящейся в компьютерной системе или на носителях компьютерных данных).

4. **Правонарушения, связанные с нарушением авторского права и смежных прав**.

5. **Дополнительные виды ответственности и санкции — покушение, соучастие или подстрекательство к совершению преступления**.

Примечательно, что Конвенция содержит положение о корпоративной ответственности (принятие мер, какие могут быть необходимы для обеспечения возможности привлечения юридических лиц к ответственности за уголовное преступление, которое совершается в его пользу любым физическим лицом, действующим индивидуально или как часть одного из органов соответствующего юридического лица и занимающим ведущее положение него на основании полномочий представлять данное юридическое лицо или права принимать решения от имени этого юридического лица или права осуществлять контроль внутри этого юридического лица).

Конвенция содержит множество процессуальных положений, посвященных таким вопросам как:

- оперативное обеспечение сохранности хранимых компьютерных данных.

[8] В понятие «детской порнографии» включаются порнографические материалы, изображающие: участие несовершеннолетнего лица в откровенных сексуальных действиях; участие лица, кажущегося несовершеннолетним, в откровенных сексуальных действиях; реалистические изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях.

- оперативное обеспечение сохранности и частичное раскрытие данных о потоках[9] информации.
- распоряжение о предъявлении: лицом — о предъявлении конкретных компьютерных данных, находящихся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на том или ином носителе компьютерных данных; поставщиком услуг[10] — о предъявлении находящихся во владении или под контролем этого поставщика услуг сведений о его абонентах[11].
- обыск и выемка хранимых компьютерных данных.
- сбор в режиме реального времени данных о потоках информации.
- перехват данных о содержании.

Указанные вопросы подробно раскрываются в соответствующих статьях Конвенции и не требуют более детального изложения или комментирования.

Вслед за европейскими странами, в рамках СНГ также заключаются межгосударственные договоры и соглашения, направленные на борьбу с компьютерной преступностью. В частности, Россия, помимо многочисленных договоров о правовой помощи, является участником Соглашения о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации.

---

[9] «Данные о потоках» означают любые компьютерные данные, относящиеся к передаче информации через посредство компьютерной системы, которые генерируются компьютерной системой, являющейся составной частью соответствующей коммуникационной цепочки, и указывают на источник, назначение, маршрут, время, дату, размер, продолжительность или тип соответствующего сетевого сервиса.

[10] «Поставщик услуг» означает: любую государственную или частную структуру, которая обеспечивает пользователям ее услуг возможность обмена информацией посредством компьютерной системы или любую другую структуру, которая осуществляет обработку или хранение компьютерных данных от имени такой службы связи или пользователей такой службы.

[11] Термин «сведения об абонентах» означает любую имеющуюся у поставщика услуг информацию о его абонентах в форме компьютерных данных или любой другой форме, кроме данных о потоках или содержании информации, с помощью которой можно установить: вид используемой коммуникационной услуги, принятые с этой целью меры технического обеспечения и период оказания услуги; личность пользователя, его почтовый или географический адрес, номера телефона и других средств доступа, сведения о выставленных ему счетах и произведенных им платежах, имеющиеся в соглашении или договоре на обслуживание; любые другие сведения о месте установки коммуникационного оборудования, имеющиеся в соглашении или договоре на обслуживание.

В соответствии с Соглашением, страны СНГ обязуются сотрудничать в целях обеспечения эффективного предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере компьютерной информации[12], а также стремиться к гармонизации национального законодательства в области борьбы с преступлениями в сфере компьютерной информации.

Подписавшие Соглашение страны СНГ признают в соответствии с национальным законодательством в качестве уголовно-наказуемых следующие деяния, если они совершены умышленно:

а) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред или тяжкие последствия;

г) незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб.

Участники Соглашения предполагают осуществлять сотрудничество в формах:

1) обмена информацией, в том числе о готовящихся или совершенных преступлениях в сфере компьютерной информации и причастных к ним физических и юридических лицах, о формах и методах предупреждения, выявления, пресечения, раскрытия и расследования преступлений в данной сфере, о способах совершения преступлений в сфере компьютерной информации, о национальном законодательстве и международных договорах, регулирующих вопросы предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере компьютерной информации;

2) исполнения запросов о проведении оперативно-розыскных мероприятий, а также процессуальных действий в соответствии с международными договорами о правовой помощи;

3) планирования и проведения скоординированных мероприятий и операций по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере компьютерной информации;

---

[12] Преступление в сфере компьютерной информации — уголовно-наказуемое деяние, предметом посягательства которого является компьютерная информация.

4) оказания содействия в подготовке и повышении квалификации кадров, в том числе путем стажировки специалистов, организации конференций, семинаров и учебных курсов;

5) создания информационных систем, обеспечивающих выполнение задач по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере компьютерной информации;

6) проведения совместных научных исследований по представляющим взаимный интерес проблемам борьбы с преступлениями в сфере компьютерной информации;

7) обмена нормативными правовыми актами, научно-технической литературой по борьбе с преступлениями в сфере компьютерной информации;

8) в других взаимоприемлемых формах.

Как видно из представленного обзора, национальное и международное законодательство стремительно развивается, и основные компьютерные правонарушения признаются таковыми в большинстве развитых стран мира. Не все они подпадают под действие уголовного законодательства. Несмотря на это, наблюдаются четкие тенденции по сближению законодательств разных стран, а также тесному международному сотрудничеству. Это и понятно: преступление, легко преодолевающее государственные границы, должно иметь адекватное правовое противодействие со стороны всех заинтересованных сторон.