

Богомолов Максим Владимирович

«Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации»

Красноярск 2002

Содержание:

Введение

Глава 1. Введение в сферу компьютерной преступности

§ 1. Криминологические последствия компьютеризации общества

§ 2. Сага о Хакере

§ 3. Некоторые мифы и заблуждения о компьютерной преступности

Глава 2. Уголовно-правовая характеристика компьютерных преступлений

§ 1. Определение некоторых компьютерных понятий

§ 2. Понятие информации

§ 3. Понятие «компьютерного преступления»

§ 4. Законодательство в сфере компьютерной информации

Глава 3. Неправомерный доступ к охраняемой законом компьютерной информации

§ 1. Неправомерный доступ

§ 2. Охраняемая законом компьютерная информация

§ 3. Информации на машинном носителе, в ЭВМ, системе ЭВМ, сети

§ 4. Обязательные последствия

§ 5. Субъективная сторона

§ 6. Субъект

Заключение

Список использованной литературы

© **Богомолов М.В. 2002.**

Глава 1. Введение в сферу компьютерной преступности [1]

§ 1. Криминологические последствия компьютеризации общества

С развитием общественно-экономических отношений объемы перерабатываемой информации постоянно увеличиваются, и если XX век многие ученые называют веком энергетики, то наступающий XXI - веком информатики. Ныне действует правило: «кто владеет информацией, тот владеет миром» [2]. Научно-технический прогресс принес человечеству такие незаменимые в современной жизни новшества, как компьютеры и Интернет. Повсеместное внедрение данных технологий повлекло за собой возникновение новых видов ресурсов – информационных. Информация обрела реальную цену и с развитием информационных технологий становится все более ценным товаром. Но новые технологии стимулировали возникновение и развитие и новых форм преступности, в

первую очередь компьютерных. Основную часть в этой сфере совершается с помощью компьютерных сетей. В последние годы специалистами замечена тенденция стремительного роста компьютерных преступлений посредством глобальной компьютерной сети Интернет [3].

«Компьютерными» принято называть преступления, в той или иной степени связанные с компьютерами и высокими технологиями, что обуславливает широко понимание термина – компьютерное преступление. Но есть, у данного термина, и более узкое понимание – уголовно-правовое, которое выделяет из общей массы преступлений, где участвуют компьютеры, преступления, посягающие на компьютерную информацию и нормальную работу ЭВМ, но данное толкование компьютерного преступления будет затронуто в следующей главе, а на данном этапе рассмотрим сложившуюся ситуацию в стране и в мире с точки зрения, общего толкования.

С этой точки зрения криминологи делят компьютерные преступления на: экономические, компьютерные преступления против личных прав и неприкосновенности частной сферы, компьютерные преступления против общественных и государственных интересов.

Наиболее опасные и распространённые – экономические компьютерные преступления – включают: компьютерное мошенничество, компьютерный экономический шпионаж и кражу программ, компьютерный саботаж, кражу “компьютерного времени”, самовольное проникновение в автоматизированную систему, традиционные экономические преступления, совершаемые с помощью компьютера.

Как отмечает профессор Н.П. Яблоков, в настоящее время распространение получили хищения в банковской деятельности с использованием компьютеров или компьютерных сетей. Этот вид хищения характеризуется тем, что преступники, воспользовавшись служебной возможностью для неправомерного доступа к компьютерной информации финансового характера, сосредоточенной в вычислительных центрах банковских учреждений, и обнаружив пробелы в деятельности ревизионных служб, осуществляют криминальные операции с указанной информацией, находящейся в ЭВМ или на машинных носителях: вносят искажения, неправильные (фальсифицированные) данные в программные выходные данные ЭВМ с последующим их использованием для хищений; устанавливают код компьютерного проникновения в электронную платежную сеть расчетов по карточкам; создают двойники платежных карточек, иногда даже моделируют бухгалтерскую систему банка или другой организации и т.д. В ряде случаев проникновение в компьютерные сети и доступ к нужной информации осуществляется с помощью различных "жучков" и прочих технических средств. В результате преступники получают возможность снимать с компьютерных счетов клиентов наличные деньги в рублевой и иностранной валюте. Совершению этих преступлений тоже предшествует определенная подготовка, характер которой зависит от степени связи правонарушителей с деятельностью вычислительного центра банка. Посторонние лица продумывают пути доступа к компьютерной системе, пытаются выяснить пароли и ключи программ. Программисты, операторы и другие работники компьютерного центра и других подразделений банка, замышляющие подобную аферу, выбирают наиболее благоприятную для ее совершения обстановку, могут создавать подставную фирму с расчетным счетом для перекачки похищенных денег и т.д. Преступная акция, по сути, складывается из начала контактных действий правонарушителя с ЭВМ или машинными носителями и снятия необходимой информации, либо денег с электронных счетов клиентов банка, их

непосредственного присвоения или перевода на счета "липовых" организаций [4].

К экономическим можно отнести получившие огромное распространение преступления нарушающие авторские права на программное обеспечение. По данным Ассоциации производителей компьютерного обеспечения, уровень компьютерного пиратства в России составляет 94%. Уровень пиратства в странах Запада существенно ниже: в Германии - 50%, в США - 35%. Однако и там убытки производителей весьма высоки - только в Европе они оцениваются в 6 млрд. долларов ежегодно. Особенно страдают американские фирмы - разработчики программного обеспечения.

В размахе компьютерного пиратства может убедиться каждый, остановившись у киосков торгующих компьютерными компакт-дисками. Во многих из них торгуют "самопальными" компакт-дисками с нелегальными копиями программ для ЭВМ, изготовленными без ведома владельцев авторских прав на эти программы. С аналогичным явлением можно столкнуться и при покупке компьютера. Ведь фирмы, занимающиеся сборкой и реализацией компьютеров, как правило, продают их с незаконно записанными в память ЭВМ чужими программами. Вот почему подавляющее большинство пользователей персональных компьютеров в нашей стране имеет дело с нелегальными программными продуктами [5].

Компьютерные преступления против личных прав и свобод и неприкосновенности частной сферы чаще всего заключаются во введении в компьютерную систему неправильных и некорректных данных о лице, незаконном собирании правильных данных (незаконными способами либо с целью, например, неправомерного контроля профсоюзных активистов), иных незаконных злоупотреблений информацией на компьютерных носителях и неправомерном разглашении информации (разглашение, например, банковской или врачебной тайны, торговля банками информацией и базами данных).

Компьютерные преступления против интересов государства и общества включают преступления против государственной и общественной безопасности, нарушение правил передачи информации за границу, дезорганизацию работы оборонных систем, злоупотребления с автоматизированными системами подсчета голосов на выборах и так далее.

Интересную мысль относительно государственной безопасности и не только, высказал **М.В. Сальников**: «говорить об обеспечении компьютерной безопасности государства возможно только в рамках обеспечения безопасности государства в целом. Обеспечивая безопасность государства, нельзя забывать и о том, что оно должно оставаться правовым. Строительство правового государства - сложный и длительный процесс, обусловленный действием множества социальных факторов. Существуют три основных условия, соблюдение которых способствует внедрению правовых начал в систему управления обществом и государством. Во-первых, общество должно быть последовательным в своем стремлении к утверждению правового государства. В противном случае почти все концепции, практические рекомендации останутся не востребуемыми. Во-вторых, необходима не только формальная, но и реальная заинтересованность общества в развитии юридической науки, в которой формируется теоретическая модель правового государства, выделяются и всесторонне изучаются его цели, задачи, основополагающие институты. И, в-третьих, сама юридическая наука не должна уходить от решения теоретических и практических вопросов становления и развития правового государства. При этом следует

подчеркнуть, что эффективное функционирование правового государства возможно только при активной роли личности в процессе становления, воспроизводства и совершенствования политических и правовых механизмов»[\[6\]](#).

Как уже говорилось, наметился стремительный рост количества преступлений совершаемых с помощью Интернет и это только начало. Интернет, как новое средство общения, обмена информацией, рынка услуг, финансовых отношений, моментального производства платежей, сегодня Internet – это глобальная компьютерная сеть, охватывающая весь мир. Он имеет около 15 миллионов абонентов в более чем 150 странах мира. Ежемесячно размер сети увеличивается на 7-10%. Internet образует как бы ядро, обеспечивающее связь различных информационных сетей, принадлежащих различным учреждениям во всем мире, одна с другой. Кроме того, Internet предоставляет уникальные возможности дешевой, надежной и конфиденциальной глобальной связи по всему миру.

Чтобы оценить криминогенный потенциал "всемирной паутины", достаточно просмотреть Уголовный кодекс. По сути, посредством эксплуатации возможностей сети могут совершаться самые разнообразные преступления. Все предусмотренные Особенной частью УК РФ составы преступлений условно разделим на две группы:

- деяния, совершение которых с помощью компьютерных сетей теоретически возможно;
- деяния, совершение которых таким способом невозможно.

Вторая группа, к сожалению, становится все меньше. Пока к ней с уверенностью можно отнести лишь такие преступления, как побои, истязание, заражение венерической болезнью и некоторые другие.

Говорить о невозможности совершения с помощью компьютерной сети, например, доведения до самоубийства, пожалуй, нельзя. А с учетом того, что постепенно компьютеризируются многие процессы жизнеобеспечения людей, нельзя исключить даже совершения убийства (преступник может, к примеру, ввести искажения в программу изготовления лекарственных препаратов и в результате добиться смерти пациента медицинского учреждения). Реально осуществление и многих других деяний, признаваемых преступными [\[7\]](#).

Итак, компьютерная преступность набирает обороты и настало время подумать, как от нее защищаться и чем с ней бороться. В настоящее время все меры противодействия компьютерным преступлениям можно подразделить на технические, организационные и правовые.

К техническим мерам можно отнести защиту от несанкционированного доступа к компьютерной системе, резервирование важных компьютерных систем, принятие конструктивных мер защиты от хищений и диверсий, обеспечение резервным электропитанием, разработку и реализацию специальных программных и аппаратных комплексов безопасности и многое другое.

К организационным мерам относятся охрана компьютерных систем, подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение

ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п. В мире и нашей стране техническим и организационным вопросам посвящено большое количество научных исследований и технических изысканий.

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. Только в последние годы появились работы по проблемам правовой борьбы с компьютерной преступностью, (в частности, это работы Ю. Батурина, В. Вехова, М. Карелиной, В. Крылова и др.) и совсем недавно отечественное законодательство встало на путь борьбы с компьютерной преступностью. И поэтому, представляется весьма важным расширить правовую и законодательную информированность специалистов и должностных лиц, заинтересованных в борьбе с компьютерными преступлениями [8].

Но как справедливо указал **В.Н. Лопатин**, «что, не смотря, на применяемые меры по законодательному закреплению прав и свобод в информационной сфере, остается немало пробелов, помогающих избегать ответственности за совершение действий, наносящих ущерб в сфере информации» [9]. С другой стороны, **Н.Л. Симарев** отметил, что «информационные технологии - это сплошное непрерывное движение. Поэтому истинную защиту информации, представленной компьютерным способом, может создать только постоянно изменяемый комплекс всех мер защиты, включая и правовое регулирование» [10].

Другие юристы предлагают определенные направления работы по криминализации, например, **С.А. Денисов** считает, что «внедрение компьютерных технологий повлекло за собой изменение в самой структуре преступности. Представляется, что нормы, содержащиеся в ст. 272-274 УК РФ, не в полной мере отражают правовую базу борьбы с компьютерными преступлениями. При сложившейся ситуации весьма актуальным кажется моделирование новых составов преступлений против собственности, в которых компьютерные системы выступают в качестве способа совершения хищения» [11].

Мысль о моделировании новых составов или внесении некоторых изменений в существующие, нужно признать правильной. Уже выявились некоторые деяния на которое следовало бы обратить внимание.

Например, как сообщали СМИ «Хакеры атаковали сайт Интернет-банка «St. George Bank». 31 августа 2001 банк подвергся атаке типа «отказ в обслуживании» (DoS), но данные о клиентах не были получены хакерами». В последнее время DoS-атаки стали одним из самых распространенных видов киберпреступности благодаря тому, что они не требуют особой квалификации. Однако надежного механизма защиты от них пока никто предложить не смог. Возможно, следует применить правовое регулирование и смоделировать новый состав?

Или же другой пример, где, опять же СМИ, стало распространителем скандала и сенсации, пугая компьютерную общественность тем, что «Жучки» в файлах Word пошлют ваши данные Гейтсу». Как выяснили специалисты, в программе Microsoft Word обнаружена недокументированная возможность отслеживать распространение документов в формате Word через Интернет с помощью скрытых "жучков", встроенных в документ. Что по сути является несанкционированным доступом к компьютерной информации. Но как пояснила

компания разработчик Microsoft, что данная возможность установлена для отслеживания нелегального распространения их собственных программных продуктов. На что общественность справедливо возмутилась, утверждая, что «даже если, на компьютере используется неоплаченная программа, никто не имеет право производить какие-либо несанкционированные действия на чужом компьютере. А все свойства программы должны явно заявляться в описании. Встает вопрос, каким способом разрешить данный вопрос? Можно ли привлечь к уголовной ответственности и кого?

Кроме проблем криминализации деяний связанных с компьютерами, существуют и проблемы непосредственной борьбы с компьютерными преступлениями уже имеющимися уголовно-правовыми средствами, и в частности, уже возникшая проблема подготовки специалистов в данной сфере. Как отметил **А.В. Аполлонский**, «существуют, по крайней мере, два фактора, определяющих данную проблему. Это - объем и характер подготовки специалистов. Проведение компьютерных расследований требует долгих часов специальной подготовки, обязательных практических навыков, в том числе и по работе со специальным оборудованием. Анализ зарубежных программ показывает, что обучение ведется весьма интенсивно, даже с учетом высокой начальной подготовки обучаемых. При подготовке специалистов по расследованию компьютерных преступлений следует помнить, что образование хакера основывается на сильном любопытстве, связанном с его увлечением. Вероятно, в силу вышесказанного в каждом из них одну из основных ролей играет психологическая подготовка, что необходимо учесть при разработке подобных отечественных программ»[\[12\]](#).

§ 2. Сага о Хакере

Компьютерные преступления обычно общество связывает с деятельностью хакеров. Но общество редко задумывается, что означает понятие «хакер» и откуда оно пришло. Пришедшее непосредственно из среды профессиональных программистов, имеет строго определенное значение, как для юриста понятие «преступления». В связи с чем, имеет смысл уяснить суть данного понятия, чтобы при дальнейшем упоминании не было недоразумений.

Просматривая большое количество статей (главным образом, в электронных журналах) о компьютерных преступлениях, нельзя не обратить внимание на тот факт, что ни в одной из них не проводится та грань, которая четко разделяет всех, так или иначе связанных с компьютерной безопасностью. В основном мнение по этому поводу либо сугубо негативное (хакеры - это преступники), либо скромно-позитивное (хакеры – «санитары леса»). На самом деле у этой проблемы существует, по меньшей мере, две стороны, положительная и отрицательная, и между ними проходит четкая граница. Эта граница разделяет всех профессионалов, связанных с информационной безопасностью, на *хакеров (hackers)* и *кракеров (crackers)*. И те, и другие, во многом занимаются решением одних и тех же задач - поиском уязвимостей в вычислительных системах и осуществлением на них атак (в частности "взлома").

Принципиальное различие между хакерами и кракерами состоит в целях, которые они преследуют. Основная задача хакера в том, чтобы, исследуя вычислительную систему, обнаружить слабые места (уязвимости) в ее системе безопасности и информировать пользователей и разработчиков системы с целью последующего устранения найденных уязвимостей. Другая задача хакера - проанализировав существующую безопасность вычислительной системы, сформулировать необходимые требования и условия

повышения уровня ее защищенности.

Основная задача же кракера состоит в непосредственном осуществлении взлома системы с целью получения несанкционированного доступа к чужой информации – обычно для ее копирования, подмены или для объявления факта взлома. Итак, кардинальное различие между хакерами и кракерами в том, что первые - исследователи компьютерной безопасности, а вторые – непосредственно преступники. Хакер в терминологии профессионалов - это специалист. В частности специализированный словарь Guy L. Steele дает такое определение:

Хакер (HACKER), сущ.

1. Индивидуум, который получает удовольствие от изучения деталей функционирования компьютерных систем и от расширения их возможностей, в отличие от большинства пользователей компьютеров, которые предпочитают знать только необходимый минимум.

2. Энтузиаст программирования; индивидуум, получающий удовольствие от самого процесса программирования, а не от теоретизирования по этому поводу.

Данная трактовка термина «хакер» отличается от принятой в средствах массовой информации, которые, собственно, и привели к подмене понятий.

Низменность мотивов кракеров и отсутствие стремления к профессиональному росту приводят к тому, что 90% из них являются «чайниками», которые взламывают плохо администрируемые системы, в основном используя чужие программы. Причем это мнение тех самых 10% профессиональных кракеров - бывших хакеров, ставших на путь нарушения закона. Их, в отличие от кракеров – «чайников», остановить которых действительно очень сложно, но, как показывает практика, отнюдь не невозможно. Очевидно, что для предотвращения возможного взлома или устранения его последствий, требуется пригласить квалифицированного специалиста по информационной безопасности - профессионального хакера.

Однако было бы несправедливо смешать в одну кучу всех кракеров, однозначно назвав их ворами. По нашему мнению, кракеров можно разделить на три следующих класса в зависимости от цели, с которой осуществляется взлом: вандалы, "шутники" и профессиональные взломщики.

· **Вандалы** - самая известная (во многом благодаря широкому распространению вирусов, а также творениям некоторых журналистов) и, надо сказать, самая малочисленная часть кракеров. Их основная цель - взломать систему для ее дальнейшего разрушения.

· **«Шутники»** - наиболее безобидная часть, основная цель которых - известность, достигаемая путем взлома компьютерных систем и внесения туда различных эффектов, выражающих их неудовлетворенное чувство юмора. К «шутникам» также можно отнести создателей вирусов с различными визуально-звуковыми эффектами (музыка, дрожание или переворачивание экрана, рисование всевозможных картинок и т. п.).

· **Взломщики** - профессиональные кракеры, пользующиеся наибольшим почетом и уважением в кракерской среде. Их основная задача - взлом компьютерной системы с серьезными целями, например с целью кражи или подмены хранящейся там информации.

Итак, исходя из изложенного, можно сказать с абсолютной уверенностью, что в сферу

действия правоохранительных органов настоящие хакеры не попадают, за исключением некоторых недоразумений, в частности с Дмитрием Скляровым. Скляров летом 2001 года на одной публичной конференции продемонстрировал изъян в системе безопасности одной из программ компании «Adobe systems», после чего был арестован сотрудниками ФБР. То есть его арестовали за то, выражаясь простым языком, что рассказал людям, что замки, которые им продают, не защитят их от воров.

§ 3. Некоторые мифы и заблуждения о компьютерной преступности

Глубокое непонимание большинством обывателей проблем, связанных с компьютерной преступностью в вычислительных системах, с течением времени сформировало определенный миф о всемогуществе кракеров и повсеместной незащитности компьютерных систем. Данный миф поддерживается и правоохранительными органами: «С помощью Internet может быть совершено любое преступление, кроме изнасилования», — заметил Дмитрий Чепчугов, начальник отдела «Р» МВД России, в своем выступлении на первой всероссийской конференции «Право и Internet: теория и практика»[\[13\]](#).

Показателен пример приводимый в юридической литературе: *В США ФБР раскрыло группу хакеров из Милуоки, которые обеспечили себе несанкционированный доступ более чем к 50-ти автоматизированным банкам данных, включая Лос-Аламосскую ядерную лабораторию, крупный раковый центр и другие, жизненно важные объекты США*[\[14\]](#).

Действительно, современные вычислительные системы (ВС) и сети общего назначения имеют серьезные проблемы с безопасностью. Но, подчеркнем, именно вычислительные системы общего назначения. Там же, где требуется обработка критической информации и обеспечение высшего уровня защиты и секретности (например, в военной области, в атомной энергетике и т. п.), используются специализированные защищенные вычислительные системы, которые (и это чрезвычайно важно!) в основном изолированы от сетей общего назначения (от сети Internet, например). Поэтому необходимо развеять первый миф, исключительно популярный в художественной литературе, кино, а также в средствах массовой информации: кракер не может проникнуть *извне* в вычислительную систему стратегического назначения (например, в ВС атомной станции или пункта управления стратегическими вооружениями).

Новую жизнь в этот миф вдохнул последний военный конфликт в Югославии. Согласно сообщениям российских СМИ, складывалось ощущение, что военные сети НАТО полностью незащитны и полный контроль над ними имеют «отважные хакеры». Естественно, если такие новости обсуждались среди профессионалов информационных технологий, то только в разделе юмора. Из этой же серии анекдот как некие «хакеры» захватили управление над **военным** спутником Великобритании, который осуществлял взаимодействие между военными судами НАТО. Этот анекдот, но уже совершенно серьезно, распространяли как новость все мировые СМИ. С сожалением можно констатировать тот факт, что у государственных органов разных стран уже стало хорошим тоном сваливать внутренние проблемы вычислительных сетей на происки неких неизвестных «хакеров».

Тем не менее, нужно говорить лишь о невозможности получения несанкционированного удаленного доступа именно *извне*. В том случае, если нанести ущерб системе вознамерится кракер из состава персонала защищенной вычислительной системы, то сложно абстрактно судить, насколько успешны будут его попытки.

В качестве примера напомним случай на Игналинской АЭС, когда местный системный программист внедрил в вычислительную систему программную закладку («тройанского коня»), которая чуть не привела к аварии на станции. Как утверждает статистика, нарушения безопасности системы собственным персоналом составляют около 90% от общего числа нарушений. Итак, критические вычислительные системы нельзя назвать неуязвимыми, но реализовать на них успешную удаленную атаку (т.е. проникнуть в систему извне) практически невозможно. В противовес данному утверждению, можно вспомнить заметки в газетах о том, как «кракеры проникли в компьютер Пентагона или НАСА». Все дело в том, что любая уважающая себя организация, будь то ЦРУ, АНБ или НАСА, имеет свои WWW- или ftp-серверы, находящиеся в открытой сети и доступные всем. И кракеры в этом случае проникали именно в них (а ни в коем случае не в секретные или закрытые сети), используя, может быть, один из простейших механизмов описываемых в компьютерной литературе.

Другим и, пожалуй, наиболее устойчивым мифом является миф о всеобщей беззащитности банковских вычислительных систем. Да, действительно, в отличие от вычислительной системы стратегического назначения, банки из-за конкурентной борьбы между собой вынуждены для обеспечения удобства и быстрого действия работы с клиентами предоставлять им возможность удаленного доступа из сетей общего пользования к своим банковским вычислительным системам. Однако, во-первых, для связи в этом случае используются защищенные криптопротоколы и разнообразные системы сетевой защиты (например, Firewall), и, во-вторых, предоставление клиенту возможности удаленного доступа отнюдь не означает, что клиент может получить доступ непосредственно к внутренней банковской сети. По мнению специалистов, зарубежные банковские ВС (про отечественные мы не говорим, так как еще не достигнут соответствующий уровень автоматизации расчетов) являются наиболее защищенными после ВС стратегического назначения.

Однако в последние годы некоторым журналистам, в том числе и отечественным, в погоне за сенсацией удалось (и не без успеха, особенно на основе реально имевшего место дела Левина, см. далее) придумать миф о всеобщей беззащитности банковских систем.

А наши банки сами поддерживают этот миф, заявляя что: «в 1993-1996 гг. было предпринято более 300 попыток проникнуть только в одну компьютерную сеть Центрального банка России»[\[15\]](#). Интересно, в какую компьютерную сеть они имели ввиду: внутреннюю стратегического назначения или веб-сервер?

В этом же духе силовые структуры пытаются преподнести «хакеров и кракеров» как самых дерзких преступников. В частности ФБР сообщает, что в их стране «совершается не менее тысячи транзакций по перекачке денег со счетов законных владельцев, совершаемых при помощи электронной техники. Сумма доходов от этих операций, ***российской и восточноевропейской мафии***, оценивается в 500 млрд. долл. США, причем российские электронщики считаются самыми опытными в мире в области компьютерных преступлений»[\[16\]](#). Интересно, куда смотрит ФБР и МВД, когда «утекают» такие деньги, да и мафия наша уже оказывается давно долларами «захлебывается». «Гордость», конечно, одолевает за наших электронщиков и мафию. Но все же думается, что данные заявления не имеют ничего общего с действительностью, а направлены получение все больших отчислений из бюджета на нужды правоохранительных органов.

В этом смысле характерно дело Левина, похитившего из американского банка в Нью-

Йорке денежные средства в размере свыше 10 млн. долларов, находясь Санкт-Петербурге. В силу большого общественного резонанса представляется важным остановиться на этом хищении более подробно. В печати делается упор на то, что это преступление было совершено чуть ли не в одиночку талантливым кракером. Однако в действительности было несколько иначе.

Например, имеется официальная версия правоохранительных органов о проведенной операции, которой, кстати, тоже не стоит сильно доверять ввиду многих неясных и нелепых мест в ней, например, такой факт: "гениальный взломщик банков" почему-то был гениален только в самом процессе взлома и вел себя, скажем, не очень умно при сокрытии своих следов и в противоборстве с правоохранительными органами.

Вторжение в систему управления денежными операциями Ситибанка было впервые замечено в июне 1994 г. В суд документы были представлены 18 августа 1995 г., и с этого момента дело получило широкую публичную огласку. Тогда же прокуратура США выдвинула обвинения против гражданина России Владимира Левина, арестованного в Лондоне.

Кракер подделывал пароли клиентов банка с целью выдать себя за владельца того или иного счета. При этом использовались счета клиентов со всего света.

Российские службы безопасности подключились к делу в 1995 г. До этого времени расследование вели специальные службы США. Была выявлена целая преступная группировка, занимавшаяся входом в компьютерную систему банка, переводом денег со счетов клиентов и получением переведенных сумм в филиалах банка по всему миру.

Счета пострадавших находились в 10-ти странах: США, Канаде, Мексике, Аргентине, Новой Зеландии, Арубе, Колумбии, Гонконге, Индонезии, Уругвае. Переводы приходили в 7 стран США, Россию, Финляндию, Германию, Нидерланды, Швейцарию и Израиль. В это дело было вовлечено в итоге 14 стран.

Организация использовала услуги кракера для проникновения в систему и перевода денежных средств со счетов клиентов в другие банки, а также "мулов" — людей, которые непосредственно получали наличную валюту из филиалов Ситибанка или других банков после поступления в них переводов. За весь период своей деятельности (с июня по октябрь 1994 г.) кракер сделал 40 попыток переводов на общую сумму более 10 млн. долларов США. Однако реальный ущерб удалось свести к 400 тыс. долларов, которые были выплачены из страховых фондов Ситибанка. *Вот так, всем сказали, что 10 млн. долларов, а оказалось 400 тысяч долларов.*

Как заявляют спецслужбы - дело было хорошо спланировано и организовано. Сначала переводы делались небольшими суммами с целью проверки качества своей работы, а затем суммы каждого перевода увеличивались до одного миллиона. При снятии крупной суммы денег наличными в банке Финляндии, согласно правилам банка, «мул» вынужден был оставить свои координаты. В качестве места своего проживания он указал Санкт-Петербург, а в графе «телефон» - тот же номер, что был засечен при фильтрации запросов и соответствовал номеру в офисе, откуда производилось проникновение. Это дало возможность связать запрос в банк с получателем как одним лицом, хотя хакер и «мул» были разными людьми. *Здесь встает один вопрос: какой вор будет оставлять на месте преступления визитку с домашним адресом? Для чего? На это есть только один ответ: правоохранительные органы на данной стадии операции использовали не совсем законные*

способы добычи информации, вследствие чего им в дальнейшем пришлось «прикрываться» явной «глупостью» «хорошо спланированного и организованного» преступления.

В результате проведенных совместных действий правоохранительных органов разных стран и службы безопасности банка были арестованы более 15 человек. Американская сторона была готова предъявить обвинения 13-ти участникам преступной группировки, большинство из которых — русские с иностранным подданством. Многие из арестованных или выданных властям США заключили сделку о признании и были осуждены по законодательству этой страны. Им вменялись в вину: банковское мошенничество (ст. 1344 титула 18 Свода законов США); мошенничество с использованием телеграфа (ст. 1343 титула 18 Свода законов США); мошенничество с использованием компьютера (ст. 1030 титула 18 Свода законов США); преступный сговор (ст. 371 титула 18 Свода законов США). А через средства массовой информации мир узнал что «талантливый хакер Владимир Левин взломав защиту Ситибанка похитил 10 миллионов долларов США».

Относительно общедоступных компьютеров глобальной сети Интернет, то можно сказать следующее. Ни одного подтвержденного факта осуществления целенаправленного получения неправомерного доступа к чужой информации в глобальной сети с помощью программных средств нет ни в России, ни за рубежом, а все известные происходили с помощью давно известного подкупа, сговора или собственной глупости пользователей. Почти каждый день «вскрываются» WWW-сервера каких-то компаний, подменой некоторых WWW-страниц, которая часто вовсе не означает полного контроля (неправомерного доступа) к Интернет- серверу, злоумышленник может вообще не иметь к нему никакого доступа, а просто подменять эти страницы с помощью переадресации. Например, группа отечественных хакеров, назвавшаяся “Антифашистским фронтом России”, провела радикальную акцию по блокированию сервера “Руспатриот. Хакерам удалось украсть у держателей сервера доменное имя ruspatriot.com путем переадресации, в результате чего каждый посетитель данного веб-адреса теперь попадает на страницу, где размещена карикатура художников Кукрыниксов “Фашизм не пройдет”, а также содержится обращение “Антифашистского фронта России” к “неуважаемым и презираемым фашистам”.

Все это позволяет нам предположить, что проблема «сетевых кракеров» в том виде, как она обычно преподносится СМИ, на самом деле отсутствует. Да, много сил должно уделяться защите компьютерных систем от «псевдохакеров», которые считают себя профессионалами, умея запускать различные «нюки» (nuke – логическая бомба, которая приводит к краху операционной системы или программного обеспечения) или подбирать пароли типа «guest» («гость») - распространенный пароль в системах общего доступа). Они способны нанести этим определенный урон. Существуют, безусловно, и более квалифицированные группы кракеров, занимающиеся, например, взломом WWW-серверов для «увечковечивания» собственного имени. Но у нас вызывает большое сомнение существование профессионалов, а тем более налаженной индустрии, которая допускает взлом любого более-менее защищенного хоста «на заказ». По собственному опыту мы можем предположить, что цена такого взлома должна быть в несколько раз больше, чем ценность находящейся там информации, поэтому в ход идут старые проверенные методы типа вербовки или подкупа.

Резюмируя, мы считаем, что никаких кракеров, специализирующихся на неправомерном доступе к Интернет-доменам за деньги или с целью использования полученной информации для собственного обогащения, не существует. Их квалификация должна быть настолько высока, что во всем мире таких людей можно без труда пересчитать, и они наверняка являются *Хакерами*, а не кракерами.

[1] Данная глава в большой степени подготовлена по материалам книги «Атака через Интернет»// Медведовский И.Д., Семьянов П.В., Платонов В.В., НПО "Мир и семья-95", 1997 г. <http://sure.org.ru/docs/hack/attack/index.html>

[2] Из доклада **В.П. Сальникова** на Международной научно-практической конференции: *Компьютерная преступность: уголовно-правовые и криминологические проблемы* //Государство и право. 2000. № 9. С. 101.

[3] Из доклада **Д.Е. Проценко** на Международной научно-практической конференции: *Компьютерная преступность: уголовно-правовые и криминологические проблемы* //Государство и право. 2000. № 9. С. 105.

[4] **Яблоков Н.П.** *Криминалистическая характеристика финансовых преступлений* // "Вестник Московского университета", Серия 11, Право, 1999. № 1

[5] **Симкин Л.** *Как остановить компьютерное пиратство?* // Российская юстиция. 1996. № 10

[6] Из доклада **М.В. Сальникова** на Международной научно-практической конференции: *Компьютерная преступность: уголовно-правовые и криминологические проблемы* //Государство и право. 2000. № 9. С. 102.

[7] **Крылов В.** *Информационные преступления - новый криминалистический объект* // Российская юстиция. 1997. № 4

[8] **В. Наумов** *Отечественное законодательство в борьбе с компьютерными преступлениями* // <http://www.hackzone.ru/articles/a5.html>

[9] Из доклада **В.Н. Лопатина** на Международной научно-практической конференции: *Компьютерная преступность: уголовно-правовые и криминологические проблемы* //Государство и право. 2000. № 9. С. 101.

[10] Из доклада **Н.Л. Симарева** на Международной научно-практической конференции: *Компьютерная преступность: уголовно-правовые и криминологические проблемы* //Государство и право. 2000. № 9. С. 103.

[11] Из доклада **С.А. Денисова** на Международной научно-практической конференции: *Компьютерная преступность: уголовно-правовые и криминологические проблемы* //Государство и право. 2000. № 9. С. 103.

[12] Из доклада **А.В. Аполлонского** на Международной научно-практической конференции: *Компьютерная преступность: уголовно-правовые и криминологические проблемы* //Государство и право. 2000. № 9. С. 106.

[13] **В. Коржов** *Право и Интернет: теория и практика* // *Computerworld (Россия), №43, 1999.* Интернет версия: <http://www2.osp.ru/cw/1999/43/06.htm>

[14] **Панфилова Е.И., Попов А.Н.** *Компьютерные преступления: Серия «Современные*

стандарты в уголовном праве и уголовном процессе» // Науч. редактор проф. Б.В. Волженкин. СПб., 1998. С. 9.

[15] **Комиссаров В.С.** *Преступления в сфере компьютерной безопасности //Юрид. мир. №2. 1998.*

[16] **Максимов В.Ю.** *Компьютерные преступления(вирусный аспект)// Ставрополь: Кн. Из-во, 1999. С. 10.*

Глава 2. Уголовно-правовая характеристика компьютерных преступлений

Анализ законодательства, регулирующего информационные отношения, показывает, что необходимо более детальное исследование правового содержания и сущности понятий, которые касаются одновременно и элементов информационных отношений и отношений, регулируемых уголовным законом. С помощью этих понятий в дальнейшем можно будет определить значимые элементы уголовной деятельности.

Понятие «компьютерного преступления» является одним из центральных в сегменте преступлений в сфере компьютерной информации, но до сих пор остается более чем не определенным. В мировой практике «... признано, что дать определение компьютерного преступления чрезвычайно сложно. Не всякое использование компьютерной системы образует состав компьютерного преступления»[1]. Есть мнение, что «сложность в формулировке этого понятия существует, как по причине невозможности выделения единого объекта преступного посягательства, так и множественности предметов преступных посягательств с точки зрения их уголовно-правовой охраны»[2]. В поисках истинного юридического значения выражения «компьютерное преступление» многие ученые и практики разошлись во мнениях более чем на четыре стороны. Относительно только объекта данного преступления в науке существует уже как минимум три мнения: сторонники первого считают, что объектом является сам компьютер (ЭВМ), второго - компьютерная информация, записанная на машинных носителях компьютера, а третьего, что общественные отношения по безопасному (законному) использованию информации являются объектом данного преступления.

Ошибочность некоторых мнений исходит из того, что суть нового явления в уголовном праве пытаются понять через призму понятий уголовной науки. Но компьютерное преступление по своей сути очень специфично и своими корнями уходит вглубь профессиональной среды специалистов в области информационных технологий. Это особый мир или отдельная страна со своими законами, понятиями, лидерами, целями и даже наказаниями. Здесь нельзя навести свой порядок, установить свой «устав». Единственный путь для уголовно-правовой науки видится в том, чтобы на основе глубокого анализа пытаться смоделировать юридические понятия и в дальнейшем грамотно регулировать отношения в данной области. Ведь не секрет, что после принятия в 1996 году нового Уголовного кодекса в информационной среде ничего не изменилось, там предпочли жить по собственным правилам и если, например, на какой-либо сервер в сети Интернет осуществлен неправомерный доступ, то собственник сервера не идет в милицию, нанимает хакера и «залатывает брешь» в защите.

Рассмотрим основные элементы информационных отношений и отношений, регулируемых уголовным законом, беря за основу профессиональные понятия ЭВМ, персональный компьютер, программное обеспечение, информация и другие.

§ 1. Определение некоторых компьютерных понятий

Весь спектр современных вычислительных систем можно разделить на три больших класса: мини-ЭВМ (включая персональные компьютеры), мейнфреймы, суперкомпьютеры. В настоящее время эти классы разнятся не столько по внешнему виду, сколько по функциональным возможностям[3]:

- супер-ЭВМ – супер электронно-вычислительная машина (super main-frame computer) предназначены для решения сложнейших задач, где требуется огромные вычислительные ресурсы, в основном в аэродинамике, метеорологии, физике высоких энергий, геофизике. Способный производить как минимум сотни миллиардов операций с плавающей точкой в секунду. Суперкомпьютеры нашли свое применение и в финансовой сфере при обработке больших объемов сделок на биржах. Их отличает высокая стоимость — от пятнадцати миллионов долларов, поэтому решение о покупке таких машин нередко принимается на государственном уровне. Таких машин не так много в мире и доступ к ним для случайных людей весьма ограничен.

- большая ЭВМ (main-frame computer) - универсальный, большой компьютер высокого уровня, предназначенный для решения задач, связанных с интенсивными вычислениями и обработкой больших объемов информации. Понятие «большая электронно-вычислительная машина» синонимично английскому термину «мейнфрейм». «Мейнфрейм» занимали господствующие позиции на компьютерном рынке до начала 1980-х годов. Наиболее крупный производитель мейнфреймов — американская фирма Ай-Би-Эм (IBM). Современные мейнфреймы отличаются исключительной надежностью, высоким быстродействием, очень большой пропускной способностью устройств ввода и вывода информации. К ним могут подсоединяться тысячи терминалов или микрокомпьютеров пользователей. Мейнфреймы используются крупнейшими корпорациями, правительственными учреждениями, банками. Стоимость мейнфреймов относительно высока: один компьютер с пакетом прикладных программ оценивается минимум в миллион долларов.

- ПЭВМ (personal computer) – персональная ЭВМ или персональный компьютер (ПК), обладающая вычислительными ресурсами и предназначена для работы только одного пользователя в один промежуток времени. С начала 1990-х годов термин «компьютер» вытеснил термин «электронная вычислительная машина» (ЭВМ), которое, в свою очередь, в 1960-х годах заменило понятие «цифровая вычислительная машина» (ЦВМ). Все эти три термина в русском языке считаются равнозначными. Само слово «компьютер» является транскрипцией английского слова computer, что означает вычислитель. Английское понятие «computer» гораздо шире, чем понятие «компьютер» в русском языке. В английском языке компьютером называют любое устройство, способное производить математические расчеты, вплоть до логарифмической линейки, но чаще в это понятие объединяют все типы вычислительных машин, как аналоговые, так и цифровые. В связи с чем, для обозначения того, что мы понимаем под словом компьютер, в англо-говорящих странах употребляют personal computer.

С одной стороны, данная классификация, не являющаяся исчерпывающей, помогает понять, что термин ЭВМ несколько шире, чем многие считают, а персональные компьютеры не единственное место, где могут быть совершены компьютерные преступления и если правоприменитель не будет стараться проникнуть в суть терминов, то для него может оказаться, что между большой ЭВМ и сетью компьютеров нет разницы. С

другой стороны, а точнее со стороны уголовно-правового регулирования, не должно быть важно, на каком типе компьютеров совершено компьютерное преступление. Важно знать, что пострадало в результате преступления.

В юридической литературе сложно найти грамотное представление о компьютере. Обычно под компьютером понимается комплекс технических средств предназначенных для производства вычислений и обработки информации – и все. Но сам по себе «комплекс технических средств» представляет собой не более чем «грудю железа». Только в монографии В.Ю. Максимова[4] было найдено действительно правильное представление, которое заключается в том, что ЭВМ, в широком смысле, является совокупностью трех составляющих:

- a) аппаратного обеспечения (hardware);
- b) программного обеспечения (software);
- c) информации (computing information).

Под *аппаратным обеспечением* (hardware) специалисты подразумевают все, что принадлежит материальной части компьютера, начиная с процессора, ОЗУ, ПЗУ, системной платы и заканчивая шлейфом и переходниками, что в комплексе образует ЭВМ.

Но что интересно, точного определения компьютера не могут дать ни специалисты, ни юристы. Сложность здесь вызывает несколько вопросов: какой комплекс оборудования можно назвать ЭВМ? С какого момента этот комплекс можно назвать ЭВМ? Какой цели должна быть подчинена работа ЭВМ? Для более полного понимания проблемы приведем одно из спорных определений: **компьютер** – *это такой комплекс оборудования, который способен выполнять команды и программы для достижения определенных вычислительных целей.* С этим определением соглашаются ряд специалистов, но они же ни как не хотят соглашаться с тем, что программируемый калькулятор «Электроника МК-61» является компьютером, хотя он полностью подходит под данное определение.

Проиллюстрируем это примером из судебной практики:

Уголовное дело № 73129 было возбуждено 9-го ноября 1998 года УРОПД ГУВД МО по факту совершения неправомерного доступа к охраняемой законом компьютерной информации в кассовых аппаратах ЧП 4001 города Павловский Посад .

Проведенным по делу расследованием установлено : в период времени с июля 1998 года, точная дата следствием не установлена, по 9-е ноября 1998 года , руководитель ЧП 4001 города Павловский Посад Московской области Титов , по предварительному сговору в группе с Ковалевой. и действуя с ней с единым умыслом , с целью сокрытия доходов от налогообложения , ежедневно , в период времени с 17-ти до 19-ти часов , в торговых палатках ЧП 4001 на улице Большая Покровка города Павловский Посад , подключали в гнезда « ЭВМ» и «Ш-К» двух контрольно-кассовых аппаратов АМС 100-Ф, являющихся разновидностью электронно-вычислительной машины , специально изготовленный самодельный прибор в виде микрокомпьютера , осуществляя доступ к компьютерной информации о проведенных через контрольно-кассовые аппараты финансовых операциях в течении текущей смены. После подключения прибора к контрольно-кассовым аппаратам и совершения неправомерного доступа к охраняемой законом компьютерной информации, в буферной памяти контрольно-кассовых аппаратов АМС 100-Ф № 29721626 и № 29721975 уничтожалась вся информация о предшествующих финансовых операциях выполненных в течении текущей смены , в том числе

информация о номере покупки и общей сумме выручки за текущую смену . Уничтожив и модифицировав информацию в буферной памяти контрольно-кассовых аппаратов в течении указанного времени, обе торговые точки ЧП 4001 продолжали свою работу накапливая информацию в буферной памяти о производимых финансовых операциях до окончания текущей смены , то есть до 21-го часа , после чего в фискальную память контрольно-кассовых аппаратов заносились измененные заниженные данные о сумме выручки за смену .

Таким образом Титов и Ковалева совершили неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе , в электронно-вычислительной машине / ЭВМ / , если это деяние повлекло уничтожение, модификацию информации , совершенное группой лиц по предварительному сговору [5].

Как видим, следователь утверждает, что контрольно-кассовый аппарат является разновидностью ЭВМ и в каком-то смысле он прав, но многие специалисты информационной сферы не согласятся с этим, мотивируя, что это лишь калькулятор, соединенный с печатающим устройством. В судебной практике пошли по наиболее легкому пути, трактуя довольно широко понятие ЭВМ, относя к ним все электронные машины способные к вычислению, в частности калькуляторы. Но можно ли считать контрольно-кассовый аппарат и калькулятор видами ЭВМ, с технической точки зрения - нет.

Представляется правильным, считать *под электронно-вычислительной машиной (компьютером) комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач.*

Есть, конечно, и другие мнения в юридической литературе определяющие ЭВМ. Например, г. Ушаков С.И., который в своей диссертации на тему компьютерного преступления заявил, что:

ЭВМ представляет собой совокупность аппаратно-технических средств и средств программирования, позволяющая производить операции над символьной и образной информацией [6].

Его определение интересно следующими заявлениями. Например, под *средствами программирования* в компьютерном мире достаточно определенно понимают языки программирования и утилиты, позволяющие создавать новые программы, но сами по себе средства программирования **не могут** вкпе с *аппаратно-техническими средствами* производить какие-либо операции. Также, общеизвестно, что ни современные компьютеры, ни компьютеры прошлого **не могут и не могли** *производить операции над символьной и образной информацией*. ЭВМ всегда «умело работать» только с оцифрованной информацией и производить операции только над цифровыми данными. Далее следует еще более интересное заявление, г. Ушаков пояснил, что он понимает под *аппаратно-техническими средствами* следующее: «под аппаратными средствами компьютерной техники понимается технические средства, используемые для обработки данных...» [7]. Тавтология данного определения понятна без комментариев. Следом возникает другая проблема, что считать под системой ЭВМ? В сфере высоких технологий компьютерной системой или системой ЭВМ называю совершенно разные вещи, например:

· для установления односторонней связи с пейджером абонента используется компьютерная система;

- в сфере экономических отношений СИСТЕМА «БАНК-КЛИЕНТ» — это компьютерная система, которая предоставляет клиенту возможность управлять банковским счетом и контролировать его, не посещая банк;
- многие современные автомобили оснащены компьютерной системой контроля работы двигателя;
- Silicon Graphics - ведущий мировой производитель мощных интерактивных компьютерных систем, в основном для решения графических и проекционных задач;
- существуют компьютерные системы для компоновки и работы с видео изображениями;
- компьютерные системы автоматизированного проектирования (САПР);
- и многое другое.

Несмотря на разнообразие в указанных примерах компьютерных системах можно найти общие черты. Итак, *ЭВМ и связанный с ней комплекс оборудования, функционирующий как единое целое, с целью решения определенного типа вычислительных задач образуют систему ЭВМ (computer system).*

Приведем пример из судебной практики:

Уголовное дело №77772 возбуждено 1 сентября 1999 года СЧ СУ при УВД ЮАО г. Москвы по признакам преступления, предусмотренного ст.272 ч. 1 УК РФ. Предварительным следствием по делу установлено:

Кроме того, Пискунов вступил с не установленным следствием лицом в сговор, направленный на совершение неправомерного доступа к охраняемой законом компьютерной информации, а также на пользование возможностями "Сотовой сети "Сонет" путем эксплуатации телефонов-двойников без оплаты владельцу оборудования сети, которым является ОАО "Персональные коммуникации", стоимости подключения и ежемесячной абонентской платы.

По своему назначению "Сотовая сеть "Сонет" предназначена для передачи речевой и иной информации. Структурно "Сотовая сеть "Сонет" выполнена на базе системы радиотелефонной связи с кодовым разделением каналов (CDMA) и представляет собой совокупность ЭВМ, соединенных каналами различной физической природы. При этом телефонные аппараты, являясь сложными электронными устройствами, управляемые хранящимися в их памяти программами, представляют из себя периферийные ЭВМ, соединенные через пространственно разнесенные базовые станции с основной ЭВМ (центральным контроллером). В память каждого официально подключенного к сети аппарата введены сведения об электронном серийном номере (ESN), являющимся уникальным в общей массе телефонных устройств, работающих в стандарте CDMA, и установленном на заводе - изготовителе телефона, и о мобильном избирательном (абонентском) номере (MIN), присваиваемым компанией - оператором сотовой связи (владельцем оборудования сети). Сведения об ESN и MIN хранятся также в памяти центрального контроллера. При выходе абонента на связь центральный контроллер проверяет соответствие комбинации двух указанных номеров, записанных в памяти телефонного аппарата, с совокупностью комбинаций, хранящихся в его памяти. В случае, если обе комбинации совпадают, то центральный контроллер "пропускает" входящий или исходящий звонок.

Телефон-двойник (клонированный телефонный аппарат) - это электронно-вычислительная машина, в программу которой без согласия владельца телефонной сети внесены такие изменения ESN и MIN, что она (телефонная сеть) воспринимает данный аппарат, как официально подключенный к ней. Обычно телефонная сеть не может отличить, какой из телефонов

(оригинальный или двойник) в конкретный момент находится на связи. Владелец телефона-двойника имеет возможность противоправно, без согласия собственника оборудования сети, вести входящие и исходящие переговоры.

Действия П***. предварительным следствием квалифицированы по ст. 272 ч. 2 УК РФ, как неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, и это деяние повлекло уничтожение, блокирование, модификацию и копирование информации, нарушение работы ЭВМ, системы ЭВМ и их сети, организованной группой[8].

В данном случае, в качестве ЭВМ выступают сотовые телефонные аппараты и центральный контроллер, а совместно с оборудованием по приему-передаче радиосигналов они образуют **систему ЭВМ**. Правда, мобильный телефон достаточно с большой натяжкой можно назвать компьютером, но это только на первый взгляд. На самом деле, такой телефон при приеме и передаче голосовых данных на основании довольно сложной программы по определенному протоколу автоматически обрабатывает кодированную компьютерную информацию. А в своем составе имеет и небольшой микропроцессор, и память, как оперативную, так и постоянную.

Следующим вопросом рассмотрения является сеть ЭВМ (computer network). Данный термин сложность в понимании и трактовке не вызывает и означает *совокупность двух и более компьютеров, соединенных между собой внешними линиями связи*. То есть, соединив хотя бы два компьютера одним кабелем через порт «LPT» или «COM» мы получим элементарную сеть ЭВМ, хотя и очень «медленную».

Под *программным обеспечением* (software) понимают такую совокупность программ, которая позволяет использовать ЭВМ как полезный инструмент, где программа – это описание алгоритма решения задачи в виде инструкций (команд), заданное на языке программирования (на машинный язык конкретной ЭВМ переводится автоматически при помощи транслятора). Как это не парадоксально, но в нашем законодательстве дано более точное определение программе:

***программа для ЭВМ** - это объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин (ЭВМ) и других компьютерных устройств с целью получения определенного результата[9].*

Программы создаются с разными целями, для решения разных задач и с разным содержанием, в связи с чем, их можно классифицировать по различным основаниям. Но обычно программы подразделяют на:

а) системные программы – это операционная система, БИОС, драйверы, всевозможные утилиты, оболочки, т.е. программы, позволяющие функционировать аппаратному обеспечению, а также обеспечивающих выполнение прикладных программ;

б) прикладные программы – служат для выполнения пользователями своих работ.

Здесь можно затронуть тему двойственности программного обеспечения. С одной стороны, программы можно воспринимать как часть компьютера, отделив от всей той информации, которую обрабатывает компьютер. С другой стороны, программное обеспечение можно вывести, как интеллектуальную составляющую, за рамки ЭВМ и тогда она встанет на одном уровне с обрабатываемой информацией. На этом моменте

акцентирует свое внимание и В.Ю. Максимов, считая, что для уголовного права более предпочтительным или даже единственным вариантом, когда аппаратное и программное обеспечение воспринимается как единое целое[10]. Чуть далее мы еще раз остановимся уже для более основательного анализа данной проблемы.

Остался третий компонент из составляющих понятие ЭВМ - *компьютерная информация* (computing information). Специалисты под КИ подразумевают, то ради чего создается программное обеспечение, работают компьютеры, т.е. такая информация, которая обрабатывается и хранится на компьютере для нужд пользователя, например, документы, оцифрованные видеофильмы и аудиозаписи, научные разработки, проекты программных продуктов, графические изображения и т.д. Но нужно не забывать, что информация имеет свою особенность, как правильно ее выразил А.В. Сорокин, который определил, что *под компьютерной информацией понимаются не сами сведения, а форма их представления в машиночитаемом виде, т.е. совокупность символов, зафиксированная в памяти компьютера, либо на машинном носителе (дискете, оптическом, магнитооптическом диске, магнитной ленте либо ином материальном носителе)* [11]. На самом деле здесь следует пояснить, в компьютере любая информация, будь-то программное обеспечение, документы или команды, представлена в виде цифровых данных, человеком не воспринимаемом. В доступную для человека информацию цифровые данные превращаются после преобразования их соответствующим программным обеспечением и вывода их на экран монитора в виде понятных человеку символов. Соответственно любая записанная на машинном носителе информация будет воспринята человеком, как результат работы компьютера и электронного преобразования программным обеспечением. Обычно среди специалистов такая информация называется - информация в электронном виде *или, как мы привыкли, компьютерная информация.*

В некоторых исследованиях для обозначения понятия компьютерная информация используется и другой термин – «машинная информация», так, в частности, В.Б. Вехов под машинной информацией понимает «информация, циркулирующая в вычислительной среде, зафиксированная на физическом носителе в форме, доступной восприятию ЭВМ, или передающаяся по телекоммуникационным каналам: сформированная в вычислительной среде информация, пересылаемая посредством электромагнитных сигналов из одной ЭВМ в другую, из ЭВМ на периферийное устройство либо на управляющий датчик оборудования»[12]. С профессиональной точки зрения данное определение правильно с одной лишь поправкой, что это информация на «низком уровне», понятная только для ЭВМ, в нее входят все данные, которые циркулируют в компьютере, в том числе и программное обеспечение. И самое главное, она перестает быть «машинной информацией», когда становится понятной человеку, т.е. после преобразования программным обеспечением. Существует и другое понимание машинной информации, как синонима термина «компьютерная информация». На данный момент термин «машинная информация» в сфере информационных технологий из-за неоднозначного понимания практически не используется. Поэтому в работе во избежание двусмысленного толкования будет применяться только термин «компьютерная информация».

На этом мы временно закончим рассматривать элементы информационных отношений со стороны информационных технологий, а рассмотрим их с юридической точки зрения.

[1] Панфилова Е.И., Попов А.Н. Указ. соч. С. 10.

[2] **А.В. Сорокин.** *Компьютерные преступления: уголовно - правовая характеристика, методика и практика раскрытия и расследования.*// http://kurgan.unets.ru/~procur/my_page.htm, 1999.

[3] По материалам «Большой Энциклопедии Кирилла и Мефодия 2001» // 2CD «Кирилл и Мефодий», 2001.

[4] **Максимов В.Ю.** Указ. соч. С. 16.

[5] Обвинительное заключение по уголовному делу № 73129// http://kurgan.unets.ru/~procur/my_page.htm

[6] **Ушаков С.И.** *Преступления в сфере обращения компьютерной информации(теория, законодательство, практика)*// Автореферат кандидатской диссертации. – Рост. –н-Д.: Рост. юр. инст. МВД РФ, 2000. С.19.

[7] **Там же.**

[8] Обвинительное заключение по уголовному делу № 77772// http://kurgan.unets.ru/~procur/my_page.htm

[9] О правовой охране программ для электронных вычислительных машин и баз данных: **Закон РФ** от 23.09.1992г. //Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. 1992. №42. Ст. 2326.

[10] **Максимов В.Ю.** Указ. соч. С. 17.

[11] **А.В. Сорокин.** Указ. соч.

[12] **Вехов В.Б.** *Компьютерные преступления. Способы совершения и раскрытия* – М.: Право и закон, 1996. С. 15. **§ 2. Понятие информации**

Трудно переоценить важность точного формализованного представления о сущности и свойствах информации как феномене, над которым осуществляется разнообразные, в том числе и уголовные, действия в информационной сфере.

Под информацией обычно понимаются – сведения об окружающем мире и протекающих в нем процессах, воспринимаемые и передаваемые человеком или специальными устройствами. В.В. Крылов считает, что *термин «информация» может интерпретироваться и как совокупность формализованных сведений (знаний), предназначенных для передачи в качестве сообщения.* Понимая под «сообщением» активные волевые действия лица по передаче информации вовне, под «знанием» упорядоченное мысленное представление о конкретном объекте, факте (или их совокупности), о способах его (их) взаимодействия и взаимосвязи с другими объектами, фактами, поддающееся описанию, приему и передаче формальным (вербальным или символьным) образом, превращаясь в «сообщение»[1]. Но законодатель в Федеральном законе «Об информации, информатизации и защите информации», в котором регулируются отношения по формированию и использованию большей части информации, так определил данное понятие:

информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Но уже в уголовном законе, как видно из описания предмета преступного воздействия в составах преступлений в области компьютерной информации, законодатель применил три

различных термина со словом «информация»: «охраняемая законом компьютерная информация», просто «информация», «охраняемая законом информация ЭВМ». Возникает вопрос, в чем разница между «компьютерной информацией» и «информацией ЭВМ» и какая информация охраняется законом? По поводу последнего вопроса в юридической периодике прозвучал весьма интересный ответ Ю. Гульбина:

Понятие «охраняемая законом компьютерная информация» весьма расплывчато и охватывает практически всю информацию на машинном носителе. Охраняется она достаточно широким кругом законодательных актов: Конституцией Российской Федерации, Гражданским кодексом РФ, законами Российской Федерации "О государственной тайне", "О правовой охране программ для электронных вычислительных машин и баз данных", "Об информации, информатизации и защите информации", "О рекламе", "О банках и банковской деятельности". И если информация не является объектом охраны одного из этих актов, то, как правило, она становится объектом охраны другого. Неохраняемой же информации практически нет[\[2\]](#).

Сомнительность подобного заявления подводит к самостоятельному анализу данных нормативных актов, которые, в том числе и Указ Президента РФ № 188 от 6.03.1997 г.[\[3\]](#), позволяют выделить действительно охраняемую информацию:

· **Информация, составляющая государственную тайну;**

· **Конфиденциальная информация:**

о Персональные данные - сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность;

о Сведения, составляющие тайну следствия и судопроизводства;

о Служебная тайна;

о Профессиональная тайна;

о Коммерческая тайна;

о Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них;

· **Документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.**

Если же первые две части (государственная тайна и конфиденциальная информация) достаточно понятны и не являются таким уж широкими понятиями, чтобы говорить о глобальной защищенности информации, документированная информация, защита которой закреплена законом «Об информации, информатизации и защите информации»[\[4\]](#) (далее Закон об информации) требует отдельного рассмотрения. В данном законе документированная информация определена следующим образом:

документированная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать[\[5\]](#).

В комментарии к Закону об информации документированная информация описывается как «организационная форма, которая определяется как единая совокупность:

а) содержания информации;

б) реквизитов, позволяющих установить источник, полноту информации, степень ее

достоверности, принадлежности и другие параметры;

с) материального носителя информации, на котором ее содержание и реквизиты закреплены»[\[6\]](#).

Значит, информация в виде электронного документа будет подходить под понятие документированная информация, если ее закрепить на компьютерном носителе информации и снабдить реквизитами, позволяющими ее идентифицировать. Информация в компьютере может находиться в трех местах: в оперативной памяти (ОЗУ), постоянной памяти (ПЗУ, чаще это устройство называют «жесткий диск») и на внешних носителях машинной информации (дискеты, компакт-диски, оптические диски и т.д.). ОЗУ не подходит для фиксации информации потому, что после выключения компьютера полностью стирается. Записанная на жестком диске или дискете информация может храниться долго, но вряд ли эту информацию можно назвать «зафиксированной», т.к. ее легко удалить, модифицировать или скопировать. Вероятно, вообще ни имеет смысла применять глагол «зафиксировать» к компьютерной информации (единственно, когда компьютерную информацию можно зафиксировать – это распечатать на принтере, но тогда она перестанет быть компьютерной), скорее ее можно «сохранить на компьютерном носителе информации». Но эта сторона компьютерной информации не принципиальная, важнее определить, с помощью каких реквизитов, возможно, идентифицировать информацию. Существующие на данный момент реквизиты электронных документов, такие как «название», «дата создания», «владелец», «объем» и «атрибуты», которые могут быть легко изменены или подделаны «без следов», не позволяют идентифицировать информацию. Но специалисты в области информационных технологий предложили уже давно используемый в компьютерном мире, способ идентификации для придания электронным документам юридической силы - электронную цифровую подпись (ЭЦП). Под ЭЦП специалисты понимают следующее:

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Надо сказать, что Закон об информации уже в 1995 году в ст. 5 определил, что:

Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.

Но нормативной базы для использования ЭЦП до текущего момента не было. 13 декабря 2001 года федеральный закон «Об электронной цифровой подписи» был принят в третьем чтении на пленарном заседании Государственной Думы. И уже на стадии второго чтения в ГосДуме, юристы и специалисты в области информационных технологий заявляли об его некоторых недостатках. Например, операторы Интернет-рынка не считают введение ЭЦП однозначно полезным. Так, в ходе подготовки к форуму "Технологии и решения для Электронной России" Член правления Союза операторов Интернет М.В. Якушев заявил: "Новый законопроект об ЭЦП содержит большое количество отсылочных норм, поэтому без соответствующего нового законодательства он будет недействителен. Поскольку законопроект предусматривает запрет на использование иностранных ЭЦП в России, его принятие приведет к изоляции России от мирового рынка". По мнению многих юристов и экспертов, закон в его нынешнем виде не готов для практического применения.

Рассмотрим некоторые понятия, вводимые новым законом. Электронная цифровая подпись определяется законом как *«реквизит электронного документа, предназначенный для его защиты от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи»*. Электронная цифровая подпись позволяет идентифицировать владельца сертификата ее ключа, а также установить отсутствие искажения информации в электронном документе. Закон обеспечивает правовые условия использования электронной цифровой подписи в электронных документах, при соблюдении которых ЭЦП в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. Также и очень кстати, законом определяется понятие документа:

документ в электронной форме отображения (электронный документ) - информация, представленная в форме набора состояний элементов электронной вычислительной техники, иных электронных средств обработки, хранения и передачи информации, могущей быть преобразованной в форму, пригодную для однозначного восприятия человеком, и имеющей атрибуты для идентификации документа;

Данный «документ в электронной форме отображения», при ближайшем рассмотрении, является видом документированной информации, а атрибутом для идентификации документа будет служить электронная цифровая подпись владельца.

Рассмотрев элементы информационных отношений и отношений, урегулированных уголовным законодательством в отдельности, приведем их в единую систему.

За базис или за глобальную составляющую информационных отношений возьмем термин «компьютерная информация». Причем, в данном случае под компьютерной информацией понимается вся информация, циркулирующая на компьютере. Хотя это утверждение на первый взгляд несколько конфликтует с описанным ранее определением компьютерной информации, но будет правильным считать именно так из-за двойственности самой информации на компьютере. Например, программное обеспечение также является компьютерной информацией, как это правильно подметил В.В. Крылов *программа для ЭВМ: ...с одной стороны, она служит инструментом воздействия на информацию; с другой стороны, она сама как совокупность команд и данных является информацией*^[7]. К тому же программное обеспечение, как обеспечивающее правильную работу компьютерной техники, также может быть предметом преступного воздействия. Итак, мы считаем, что предмет преступного посягательства преступлений в сфере компьютерной информации должен выглядеть так:

· ***Компьютерная информация*** - вся информация, циркулирующая на компьютере или в сети компьютеров, как записанная на машинных носителях, так и загруженная в оперативную память компьютера.

о ***Информация*** - сведения о лицах, предметах, фактах, событиях, явлениях и процессах, циркулирующая на компьютере.

§ ***Охраняемая законом информация*** – информация, поставленная под защиту следующими законами: Конституцией Российской Федерации, Гражданским кодексом РФ, законами Российской Федерации "О государственной тайне", "О правовой охране программ для электронных вычислительных машин и баз данных", "Об информации, информатизации и защите информации" и другие:

- *Информация, отнесенная к государственной тайне;*
- *Конфиденциальная информация;*
- *Документированная информация.*

о **Программное обеспечение** – все программное обеспечение и в любом виде (эксплуатируемое или в дистрибутивном виде).

[1] **Крылов В.В.** *Информация как элемент криминальной деятельности* // Вестник Московского университета, Серия 11, Право, 1998. № 4. С. 54.

[2] **Гульбин Ю.** *Преступления в сфере компьютерной информации* // Российская юстиция. 1997. № 10

[3] Об утверждении перечня сведений конфиденциального характера: **Указ Президента РФ** от 06.03.1997 г. № 188 // Собрание законодательства РФ. 1997. №10. Ст. 1127.

[4] Об информации, информатизации и защите информации: **Федеральный закон** от 20.02.1995 г. // Собрание законодательства РФ. 1995. № 8. Ст. 609.

[5] Нужно отметить, что смысл понятия «идентификация» в тексте закона отличается от принятого в криминалистике.

[6] **Федеральный закон** «Об информации, информатизации и защите информации»: Комментарий. М.1996. С.16.

[7] **Крылов В.В.** *Информация как элемент криминальной деятельности* // Вестник Московского университета, Серия 11, Право, 1998. № 4. С. 59.

§ 3. Понятие «компьютерного преступления»

Разобравшись с некоторыми вспомогательными понятиями, следует перейти к основному понятию: «компьютерного преступления». Есть точка зрения, в рамках которой к «компьютерным преступлениям» относятся все противоправные деяния, так или иначе связанные с компьютерной техникой[1]. Для такого подхода безразлично, в качестве чего задействована в правонарушении названная техника: объекта, предмета, орудия или средства; что именно страдает в итоге такового: аппаратная часть, программное обеспечение, база данных; кто конкретно из соучастников и каким образом использовал ЭВМ и так далее. При таком понимании термина уравниваются в юридическом смысле незаконное копирование авторского программного продукта, блокирование компьютерной системы Министерства обороны с целью подрыва обороноспособности страны, кража принтера и убийство путем нанесения удара данным принтером по голове потерпевшего. Данные деяния можно с успехом квалифицировать и по другим составам преступлений, описанным в УК РФ.

Имеется и более узкие по объекту регулирования определения. Так В.Б. Вехов считает, что *под компьютерными преступлениями следует понимать предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства. В данном случае в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть*[2]. Эту точку зрения восприняли «на ура» господа криминалисты ввиду его ясности по объекту, предмету и орудию (т.к. все «свалено» в одну

кучу и не требуется разграничения), что соответственно сказалось и на практике применения уголовного законодательства[3].

Но рассматриваемое определение опять же слишком широко трактует компьютерные преступления, так к ним можно тогда отнести оплату покупки при помощи поддельной пластиковой кредитной карточки (так называемое "компьютерное мошенничество") или незаконный перевод денежной суммы с одного счета в банке на другой ("компьютерная кража"), несанкционированный сбор информации с целью использования ее для ослабления какой-либо организации или даже государства ("компьютерный шпионаж") и другие, которые практически не отличаются от своих «собратьев»: мошенничества, кражи и шпионажа. Отличает лишь использование в той или иной степени компьютерной техники при совершении преступления. Действительно, как отмечают некоторые юристы, это наиболее простой и «очевидный» путь для уголовного права по которому пошли некоторые страны Европы и Америки[4]. Однако и эти преступления вполне подпадают под соответствующие статьи УК РФ. На квалификацию кражи, к примеру, не будет влиять, совершена она при помощи отмычки, куска провода или же персонального компьютера (между тем, около половины всех преступлений, связанных с использованием ЭВМ, - именно кражи денежных средств). С уголовно-правовой точки зрения эти орудия и средства совершенно равноценны и их фактическое своеобразие может быть только учтено судом при индивидуализации наказания во время вынесения обвинительного приговора[5]. С этим согласен и профессор С.В. Бородин: *В тех случаях, когда компьютерная аппаратура является предметом преступления против собственности, соответственно ее хищение, уничтожение или повреждение подлежит квалификации по ст.ст. 158-168 УК РФ. Но дело в том, что информационная структура (программы и информация) не может быть предметом преступления против собственности, поскольку машинная информация не отвечает ни одному из основных критериев предмета преступления против собственности, в частности не обладает физическим признаком. Что касается компьютера как орудия преступления, то его следует рассматривать в ряду таких средств, как оружие или транспортные средства. В этом смысле использования компьютера имеет прикладное значение при совершении преступлений, например хищения денежных средств или сокрытие налогов. Такие действия не рассматриваются в качестве самостоятельных преступлений, а подлежат квалификации по другим статьям УК в соответствии с объектом посягательства*[6].

Но ряд авторов еще более сужают круг компьютерных преступлений, оставляя только те, которые посягают непосредственно на компьютерную информацию. Но расходятся во мнениях относительного того, чем является информация, объектом или предметом противоправного деяния? Сторонники позиции, где информация – это объект преступления, считают, что информация, в том числе и компьютерная, является общественным благом, т.к. терпит ущерб при незаконном уничтожении или модификации, с этим сложно не согласиться. Но компьютерная информация может подвергнуться и незаконному копированию (например, конфиденциальная информация) и блокированию, при этом сама по себе информация ни каким образом не пострадает. А объект преступления должен нести ущерб всегда, иначе, в чем бы тогда состояло преступление? Что же происходит в этих двух случаях? Что же тогда терпит урон? В первом случае страдают отношения законного обладателя информации по ее монопольному использованию, а во втором, страдают отношения по непосредственному законному использованию. Итак, приходим к выводу, что сама по себе компьютерная информация не

всегда терпит ущерб, но во всех случаях страдают некоторые отношения по ее использованию.

Итак, на данном этапе можно утверждать, что компьютерная информация выступает в качестве **предмета** компьютерных преступлений в уголовно-правовом понимании. Затронем несколько иную проблему. В юридической литературе иногда высказывается такой вопрос: *является ли компьютерная информация только лишь предметом преступлений такого вида или же она может выступать и их средством, когда электронно-вычислительная техника используется с целью совершения другого противоправного посягательства на иной объект?* Ответ обычно звучит отрицательный. Например А.В. Сорокин считает, что *«принять, что информация является также средством совершения других преступлений, означало бы слишком расширить рамки понятия «компьютерное преступление» и затруднить работу, как законодателя, так и правоприменителя»*[7]. С технической точки зрения, компьютерная информация действительно является *средством* действия (и не только преступного) в рамках компьютерной системы, но мы тогда не должны отделять ее от самой ЭВМ. То есть *средством* в техническом и юридическом смысле информация будет только в совокупности с компьютером, а не отдельно от него. В связи с чем, вопрос можно считать исчерпанным и при квалификации преступлений, где ЭВМ является средством, воспринимать ЭВМ как комплекс аппаратного и программного обеспечения.

Хотя уже вроде поставлены точки над «i» и уже можно было бы дать окончательное определение, но даже здесь есть различные точки зрения. Например, В.С. Комиссаров предлагает определять *преступления в сфере компьютерной информации как умышленные общественно опасные деяния (действие или бездействие), причиняющие вред либо создающие угрозу причинения вреда общественным отношениям, регламентирующим безопасное производство, хранение, использование или распространение информации и информационных ресурсов либо их защиту*[8]. На первый взгляд, очень точное и правильное определение, НО при анализе его видно, что В.С. Комиссаров имеет в виду некие *«общественные отношения, регламентирующие безопасное производство, хранение, использование и распространение информации и информационных ресурсов либо их защиту»*. Обычно под такими отношениями понимают нормативные акты или правила эксплуатации, т.е. при незаконном копировании информации страдают отношения между законным обладателем и государством (обществом), которое через нормативные акты регламентировало ему монопольное ее использование. Получается не совсем то, что хотели.

Есть точка зрения, на наш взгляд более правильная и высказанная В. Ю. Максимовым, который компьютерные преступления определяет *«как такую разновидность информационных преступлений, такие противоправные, виновно совершенные, наказуемые в уголовном порядке общественно опасные деяния, предмет которых является компьютерная информация, а объектом - отношения по ее нормальному, безопасному использованию»*[9]. Но и здесь не все «гладко». Смущает лишь одно: безопасное использование компьютерной информации. В уголовно-правовом смысле безопасное использование, например, огня или ядерной энергии, не может быть сравнено с безопасным использованием компьютерной информации. Специфика информации ЭВМ в том, что удаление, копирование, создание или модифицирование не может быть опасным или безопасным как для законного обладателя, так и для правонарушителя. Это лишь

переход информации из одного состояния в другое. Вместо слова «безопасное» следует использовать – «законное» использование информации, т.к. только законный обладатель информации должен иметь возможность удалять, копировать, создавать или модифицировать информацию.

Итак, с учетом вышесказанного можно дать следующее определение:

***Компьютерное преступление** – это противоправное, виновно совершенное, наказуемое в уголовном порядке общественно опасное деяние, причиняющие вред либо создающие угрозу причинения вреда общественным отношениям по законному использованию компьютерной информации.*

[1] Максимов В.Ю. Указ. соч. сс. 20.

[2] Вехов В.Б. Указ. соч. С. 17.

[3] А.В. Сорокин. Указ. соч.

[4] Панфилова Е.И., Попов А.Н. Указ. соч. С. 34.

[5] Максимов В.Ю. Указ. соч. С. 22.

[6] *Комментарий к Уголовному кодексу РФ*// Отв. ред. А.В. Наумов. – М.: Юристъ, 1997. С. 662.

[7] А.В. Сорокин. Указ. соч.

[8] Комиссаров В.С. *Преступления в сфере компьютерной безопасности* //Юрид. мир. №2. 1998.

[9] Максимов В.Ю. Указ. соч. С. 23.

§ 4. Законодательство в сфере компьютерной информации

Широкая сфера применения компьютерных технологий затрагивает чаще уже известные виды преступлений, но только совершенные в новой форме или новым способом. Как мы уже указывали ранее, многие из них можно было бы квалифицировать по традиционным составам, но исключительные особенности таких деяний не позволяют в полной мере этого сделать. В связи с чем, задача уголовного права в формулировании наиболее общих, характерных для большинства таких деяний совокупностей их признаков, характеризующих все их стороны, т.е. выделение из массы совершенных преступных акций составов преступлений, а также оценка их с точки зрения права.

Мировая уголовно-правовая практика в зависимости от традиций законодательства той или иной страны идет в решении вышеназванной проблемы двумя путями: или путем дополнения традиционных составов преступлений новыми, в данном случае – компьютерными, аспектами, или же путем формирования новых норм и институтов права, объединенных единым специфичным объектом преступления.

Российское уголовное право и законодательство всегда шло по второму пути развития, беря за основу криминализации новых разновидностей преступлений признак их объекта и находя для него место в уголовно-правовом «дереве объектов» [1]. Хотя некоторые теоретики (Ю.М. Батулин и А.М. Жодзинский) предлагали объединить пути, внося в Уголовный кодекс самостоятельные статьи, а ряд статей дополнить квалифицирующими признаками [2].

Но до изменений в УК требовалось еще создать базу нормативных актов, где были бы определены основные термины и понятия в области компьютерной информации, урегулированы вопросы ее распространения, охраны авторских прав, имущественные и неимущественные отношения, возникающие в связи с созданием, правовой охраной и использованием программного обеспечения и новых информационных технологий. Также необходимо было осуществить законодательное раскрытие понятий информационной безопасности и международного информационного обмена. До 1992 г. вообще не было законодательно установлена какая-либо защита отношений в сфере высоких технологий.

23 сентября 1992 г. принимается **Закон Российской Федерации № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных»**[\[3\]](#) (далее – Закон о защите программ). Основной идеей этого закона, а также принятого одновременно с ним **Закона Российской Федерации № 3526-1 «О правовой охране топологий интегральных микросхем»**[\[4\]](#) (далее – Закон о защите микросхем) являлось урегулирование отношений в сфере защиты прав авторов и разработчиков программно-технического обеспечения.

В Законе о правовой охране программ впервые в отечественной законодательной практике были зафиксированы важнейшие понятия и правовые конструкции, отражающие представления законодателя об элементах охраняемой сферы. Давались определения целому ряду терминов, "программа для ЭВМ", "база данных", "модификации программы" и другие, положивших основу развитию правовой терминологии в данной области[\[5\]](#).

Далее **Закон Российской Федерации «Об авторском праве и смежных правах»**[\[6\]](#), принятый в 1993 г., регулирует отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм, исполнений, постановок, передач организаций эфирного или кабельного вещания (смежные права).

Закон Российской Федерации «О государственной тайне»[\[7\]](#) (далее – Закон о гостайне), принятый в 1993 г., урегулировал отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Законом «Об обязательном экземпляре документов»[\[8\]](#), принятым в 1993 г., впервые определяется понятие документа.

Принятый в 1994 г. **Гражданский кодекс Российской Федерации**[\[9\]](#) впервые (ст. 128) отнес к объектам гражданских прав информацию и результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность). В статье 139 законодатель конкретизировал свои представления об информационных отношениях, включив в эту сферу вопросы, связанные со служебной и коммерческой тайной.

Закон «О связи»[\[10\]](#), принятый в 1995 г., установил правовую основу деятельности в области связи, определил полномочия органов государственной власти, по регулированию указанной деятельности, а также права и обязанности физических и юридических лиц, участвующих в указанной деятельности или пользующихся услугами связи.

Федеральный закон «Об информации, информатизации и защите информации» принятый в 1995 г., регулирует отношения, возникающие при:

- формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;
- создании и использовании информационных технологий и средств их обеспечения;
- защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

Закон не затрагивает отношений, регулируемых законодательством об авторском праве и смежных правах.

Целью **Федерального закона «Об участии в международном информационном обмене»** [11], принятого в 1995 г., является создание условий для эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства, защита интересов Российской Федерации, субъектов Российской Федерации и муниципальных образований при международном информационном обмене, защита интересов, прав и свобод физических и юридических лиц при международном информационном обмене. В дополнение к определениям, установленным ранее, данный Закон ввел ряд новых определений, таких, как "массовая информация", "информационные ресурсы", "информационные продукты", "информационные услуги" и др.

Следует также упомянуть Указы Президента РФ, которые касаются, прежде всего, вопросов формирования государственной политики в сфере информатизации, (включая организационные механизмы), создания системы правовой информации и информационно-правового сотрудничества с государствами СНГ, обеспечения информацией органов государственной власти, мер по защите информации (в частности, шифрования).

Логическим развитием правовой системы, создающей условия безопасности компьютерной информации, стала разработка в УК РФ 1996 года группы статей, предусматривающих основания уголовной ответственности за так называемые компьютерные преступления. Но затронем с начало немного предыстории принятия УК РФ, чтобы понять насколько сложной была проделанная работа.

Основываясь на достаточно устаревших, на рассматриваемый момент представлениях машинных данных как об одном из производственных ресурсов, разработчики представили первый проект (1994г.) криминализации компьютерных преступлений в виде внесения изменений и дополнений в действующий УК РСФСР, который состояла из шести следующих статей:

- ст. 152-3. «Незаконное овладение программами для ЭВМ, файлами и базами данных»;
- ст. 152-4. «Фальсификация или уничтожение информации в автоматизированной системе»;
- ст. 152-5. «Незаконное проникновение в АИС, совершенное путем незаконного завладения парольно-ключевой информацией, нарушение порядка доступа или обхода механизмов программной защиты информации с целью ее несанкционированного копирования, изменения или уничтожения»;

- ст. 152-6. «Внесение или распространение «компьютерного вируса»;
- ст. 152-7. «Нарушение правил, обеспечивающих безопасность АИС»;
- ст. 152-8. «Промышленный шпионаж с использованием ЭВМ».

Но проект не был реализован ввиду постановки новой задачи в виде формирования уже в рамках нового Уголовного кодекса преступлений в области компьютерной информации. Минюстом России и Государственно-правовым управлением Президента РФ был разработан проект нового УК, два варианта которого были опубликованы в 1994[12] и 1995[13] гг., где содержалась глава «**Компьютерные преступления**». Заслугой авторов было верное определение родового объекта. Считая, что последствия неправомерного использования информации ЭВМ могут быть самыми разнообразными, поместили компьютерные преступления в раздел IX «**Преступления против общественной безопасности и общественного порядка**». Оба варианта проекта в главе «компьютерные преступления» между собой не сильно отличались. А в отношении самого первого проекта изменений и дополнений, при некоторых различиях в последовательности расположения статей и в используемой терминологии, количество и сущность остались теми же. Юристами и специалистами в области информационных технологий было указано на существенные недостатки, в частности, на отсутствие единой правовой концепции в главе, недостаточную связь с отраслевыми законами, слабую проработку терминологии и стилистику[14].

После интенсивной работы думской согласительной комиссии по доработке проекта УК РФ, глава предстала в следующем виде:

Глава 28. Преступления в сфере компьютерной информации.

Статья 268. Неправомерный доступ к компьютерной информации.

Статья 269. Создание, использование и распространение вирусных программ.

Статья 270. Нарушение правил эксплуатации компьютерной системы или сети.

Таким образом, были внесены значительные изменения. Несколько статей объединены в одну, изменилась терминология, расширился список опасных деяний с компьютерными вирусами и др. Однако и на этом работа над главой 28 не была остановлена, в феврале 1996 г. Президент РФ возвращает проект УК на последнюю доработку, в итоге которой глава, со многими изменениями и поправками, предстала в конечном варианте и 24 мая 1996 г. УК РФ был принят.

Итак, компьютерные преступления, определенные в главе 28 УК РФ, как уголовно наказуемые деяния, отнесены законодателем к посягающим на общественную безопасность и общественный порядок и помещены в раздел IX «Преступления против общественной безопасности и общественного порядка». Что можно считать совершенно оправданным, как мы указывали ранее, последствия неправомерного использования информации могут быть самыми разнообразными: это не только нарушение неприкосновенности интеллектуальной собственности, но и разглашение сведений о частной жизни граждан, имущественный ущерб в виде прямых убытков и неполученных доходов, потеря репутации фирмы, различные виды нарушений нормальной деятельности предприятия, отрасли и т.д.

Неявная (большей частью) бланкетность диспозиций уголовного закона,

устанавливающего ответственность за компьютерные преступления, требует при их квалификации применения законодательства, регулирующего информационные правоотношения, и, соответственно, терминологии, используемой этой отраслью законодательства[15]. Однако, как правильно указал В.В. Крылов, *прямое использование в криминалистической практике представления о компьютерной информации, изложенного в Законе об информации, без учета уточненной в УК РФ позиции законодателя было бы не корректным*[16]. Это означает, что понятие компьютерной информации нужно воспринять комплексно из всех законов, затрагивающих информацию на ЭВМ, но с точки зрения диспозиций главы 28, как и было описано в § 2 данной работы.

В юридической литературе высказывается мнение о слабой проработке в статьях о компьютерных преступлениях вопроса о последствиях. В частности, совершенно справедливо отмечает Г.П. Новоселов, что *«сам факт уничтожения, блокирования, модификации, копирования охраняемой законом информации причиняет ущерб владельцу информации... Но серьезные препятствия в пользовании владельцем своей информацией могут возникнуть и в результате нарушения работы ЭВМ, системы ЭВМ, их сети, а стало быть, и такие последствия незаконного деяния должны влечь уголовную ответственность ... Вместе с тем применительно к наказуемости нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети упоминается о последствиях в виде уничтожения, блокирования или модификации информации, но ничего не говорится о нарушении работы ЭВМ, системы ЭВМ, их сети. Не совсем понятно, почему при нарушении данных правил, если оно повлекло уничтожение информации, виновный может быть привлечен к уголовной ответственности, а при последствиях в виде нарушения работы ЭВМ – не может»*[17].

Также нужно сказать о непоследовательном подходе к формированию квалифицирующего признака о неосторожном причинении тяжких последствий. Такой признак предусмотрен в двух статьях 273 и 274 УК РФ, но не предусмотрен при неправомерном доступе к информации. Нужно согласиться с Г.П. Новоселовым, что такое решение законодателя нельзя признать верным, потому что неосторожное причинение тяжких последствий в равной степени может быть следствием всех трех незаконных деяний.

[1] **Максимов В.Ю.** Указ. соч. С. 27.

[2] **Батурин Ю.М., Жодзишский А.М.** *Компьютерная преступность и компьютерная безопасность.* – М.: Юрид. лит., 1991. С. 28.

[3] **Закон РФ** «О правовой охране программ для ЭВМ и баз данных» от 23.09.92 №3526-1 // Российская газета, № 230. 21.10.92.

[4] **Закон РФ** «О правовой охране топологий интегральных микросхем» от 23.09.92 №3523-1 // Российская газета, № 229. 20.10.92.

[5] **Крылов В.В.** *Информационные компьютерные преступления*// М.: Изд. Инфра-М-Норма, 1997. С. 13.

[6] **Закон РФ** «Об авторском праве и смежных правах» от 09.07.93 № 5351-1 // Российская газета. № 147. 3 АВГ. 1993

[7] **Закон РФ** «О государственной тайне» от 21.07.93 № 5485-1// Российская газета. № 182. 21.09.93

- [8] **Закон РФ** «Об обязательном экземпляре документов» от 23.11.94 № 77-ФЗ // Российская газета. № N 11-12. 17.01.95
- [9] Гражданский кодекс Российской Федерации (часть первая) от 21.10.94 г. № 51-ФЗ // Российская газета. № 238-239. 08.12.94
- [10] **Закон РФ** «О связи» от 21.07.93 № 5485-1// Российская газета. № 211 от 14.09.93
- [11] Об участии в международном информационном обмене: **Федеральный закон** от 05.06.96 № 85-ФЗ. // Российская газета. № 129. 11.07.96
- [12] Уголовный кодекс РФ. Особенная часть. Проект // Юридический вестник. 1994. № 22-23.
- [13] Уголовный кодекс РФ. Проект // Юридический вестник. 1995. № 7-8.
- [14] **Максимов В.Ю.** Указ. соч. С. 33.
- [15] **Крылов В.В.** Указ. соч. С. 11.
- [16] **Крылов В.В.** *Информация как элемент криминальной деятельности* // Вестник Московского университета, Серия 11, Право, 1998. № 4. с. 54.
- [17] *Уголовное право. Особенная часть*//Отв. ред.: **И.Я. Козаченко, З.А. Незнамова, Г.П. Новоселов**- М.: Изд. НОРМА-Инфра*М, 1998. С.556.

Глава 3. Неправомерный доступ к охраняемой законом компьютерной информации

Сегодня применение нормы, содержащейся в ст.272 УК РФ, ограничено правовой и практической неразработанностью вопросов, связанных с использованием и охраной компьютерной информации, но правовая основа уже заложена.

Воспроизведем диспозицию **ст. 272 УК РФ**

1. 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;

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

На наш взгляд, не имеет смысла сухо констатировать состав данного преступления, как это сделано в большинстве комментариев к Уголовному кодексу. Цель данного параграфа – найти четкие рамки законодательной конструкции для практического применения.

Определить экстремум далеко неоднозначных понятий и приблизить их к жизненным реалиям.

Рассмотрим, какой смысл таит в себе диспозиция данной статьи.

§ 1. Неправомерный доступ

В самом начале встречается неоднозначное понятие «неправомерный доступ». Как показал анализ статей Уголовного кодекса РФ, этот термин используется дважды: в контекстах «ограничение доступа на рынок» (ст. 178 «Монополистические действия и ограничения

конкуренции») и «неправомерный доступ к компьютерной информации». Кроме того, с точки зрения толкования, в последнем случае у данного термина двойной смысл: технический и юридический.

В техническом плане *неправомерный доступ* означает доступ к информации (что включает возможность: ознакомления, копирования, уничтожения и модификации информации), полученный вследствие несанкционированного преодоления программной, аппаратной или комплексной защиты. Такой защитой может быть элементарный пароль на файле документа или вход администратора на сервер с помощью магнитной карты-ключа и ввода усложненного 16 символьного пароля. Несанкционированное преодоление защиты и в первом, и во втором случае будет с компьютерной точки зрения «неправомерным доступом» к защищенной информации. Но если для доступа к информации не предусмотрена защита, то неправомерным такой доступ назвать нельзя. Например, если информация конфиденциального характера расположена на жестком диске компьютера, подключенного к локальной компьютерной сети и доступ к этому компьютеру открыт с любого компьютера, подключенного к данной сети, то можно смело сказать, что данные общедоступны, а не конфиденциальны.

Но с юридической точки зрения все намного сложнее. Хотя господа криминалисты восприняли формулировку, близкую к технической:

неправомерным признается доступ не обладающего правами на это лица к компьютерной информации, в отношении которой принимаются специальные меры защиты, ограничивающие круг лиц, имеющих доступ[\[1\]](#).

Однако, в ней больше вопросов, чем ответов. Например, в силу чего лицо может обладать правами, в силу специальных мер защиты или в силу закона? На каком основании и кто может такие меры устанавливать? и т.д. Да и с понятием *доступа* у криминалистов не все «гладко».

Под доступом к компьютерной информации подразумевается любая форма проникновения в источник информации с использованием средств электронно-вычислительной техники, позволяющая производить манипуляции с полученной компьютерной информацией[\[2\]](#).

Что может означать слово «проникновение»? А **правомерный** доступ тоже будет *проникновением*?! Само слова «проникновение» несет в себе аспект неправомерности, что не укладывается в смысл законного использования информации. А что подразумевается под «источником информации» - человек, документ или жесткий диск компьютера? И последнее, *проникновение в источник информации с использованием средств электронно-вычислительной техники*, можно совершить, например, таким образом: предположим, имеется секретная информация в форме обыкновенного бумажного документа, лежащего на столе в некотором кабинете, дверь которого закрыта на современный электронный замок с цифровым паролем. К двери подходит злоумышленник, вскрывает крышку замка и к определенным проводам подключает микрокомпьютер, с помощью небольшой программы компьютер в считанные минуты подбирает пароль и вот кабинет открыт. Налицо *проникновение с использованием средств электронно-вычислительной техники*, осталось сделать два шага к источнику информации. Практически сценарий «голивудского боевика», но никак не состав преступления предусмотренный ст. 272 УК РФ, т.к. информация не компьютерная, а закрепленная на бумажном носителе и проникновение

произведено не в ЭВМ, а кабинет.

Но как ни странно, это же определение *доступа* дается в одном из комментариев к Уголовному кодексу [3]. Теперь становится, понятна широта размаха и некомпетентность правоохранительных органов при квалификации, как компьютерное преступление, всех деяний так или иначе связанные с компьютером. Рассмотрим один из таких примеров судебной практики:

Уголовное дело № 011678 возбуждено 8 октября 1999 года г. Новгороде по признакам преступления, предусмотренного ст. 242 и ч.2 ст.272 УК РФ. Из обвинительного заключения выяснено, что Федоров, в рамках договора о совместной деятельности с ООО «Технотрон», получил для осуществления наладки доступа к сети Интернет компьютер г. Борисова с находящимися в нем именем пользователя и паролем доступа для работы в сети Интернет (Internet).

9 сентября 1999 года Федоров из офиса ООО «Технотрон», используя компьютер, без ведома и разрешения владельца, вышел в глобальную сеть Интернет и произвел несанкционированную модификацию программы публичного поискового сервера Новгородского Государственного университета <http://search.novgorod.ru>, разместив в одном из разделов данной программы гиперссылку на расположенный по адресу <http://www.novgorod.net/~apache/xxx/image> графический файл «ева002.ДжейПиДжи» (eva002.jpg). Данное деяние квалифицировано как преступление, предусмотренное ч. 2 ст. 272 УК РФ – неправомерный доступ к охраняемой законом компьютерной информации, то есть информации в системе ЭВМ и их сети, если это деяние повлекло модификацию информации, совершенное лицом, имеющим доступ к ЭВМ, системе ЭВМ и их сети.

Действия Федорова по размещению на ВЭБ – странице по адресу <http://www.novgorod.net/~apache> и в публичном поисковом сервере НовГУ по адресу <http://search.novgorod.ru> изображений, признанных искусствоведческой экспертизой порнографическими, квалифицированы как преступление, предусмотренное ст. 242 УК РФ – незаконные распространение и рекламирование порнографических материалов [4].

На данном этапе рассмотрим в этом примере только наличие неправомерного доступа. Из вышеприведенного можно заключить, что следователь указывает на два случая неправомерного доступа: во-первых, Федоров, произвел неправомерный доступ к *имени пользователя и паролю*, выйдя в сеть Интернет; во-вторых, *произвел несанкционированную модификацию программы публичного поискового сервера Новгородского Государственного университета*.

В первом случае специалисты, вероятно, не пояснили следователю, что для осуществления ремонта в виде отладки доступа в Интернет совершенно официально требуется *имя и пароль абонента*, а для проверки ремонта требуется непосредственный выход в Интернет. Поэтому совершенно недопустимо говорить, что Федоров *без ведома и разрешения владельца вышел в глобальную сеть Интернет*, можно лишь предположить, что он пробыл в сети Интернет больше, чем требуется для отладки, тем самым, нанеся Борисову некоторый материальный ущерб, который может быть возмещен с помощью гражданского иска.

Во втором случае, так называемая «несанкционированная модификация» поисковой программы состояла лишь в том, что Федоров ввел гиперссылку [5] в качестве ключевого слова для поиска - то есть, попросту говоря, поискал адрес своей персональной страницы через поисковую систему НовГУ, что мог сделать любой желающий. Поисковая система НовГУ была устроена так, что публично показывала на своей странице несколько

последних запросов [6]. Поэтому адрес сайта Федорова высветился как гиперссылка в этом списке. То есть, с технической стороны, никакой модификации программы не было, а Федоров лишь использовал *возможности* публичного поискового сервера Новгородского Государственного университета, предоставляемые *всем желающим*, сама программа продолжала работать в обычном режиме. Таким образом, модификации, а тем более несанкционированной, установить в действиях Федорова нельзя. Итак, можно говорить об отсутствии какого-либо **неправомерного доступа** в действиях инкриминированных Федорову.

Из вышеописанного анализа можно сделать вывод о слабом представлении понятия «неправомерного доступа», как в теории, так и на практике. В связи с чем, следует подробно рассмотреть данное понятие и в первую очередь нужно остановиться на определении понятия «доступа». Примерное представление законодателя о смысле данного понятия можно найти лишь в п.5 ст. 2 Закона о гостайне:

доступ к сведениям, составляющим государственную тайну, - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

Если отойти от частного случая доступа и перефразировать данное определение в более общей форме, получится, что

доступ к информации – это санкционированное владельцем или собственником ознакомление конкретного лица с информацией.

Что же понимать тогда под *неправомерным доступом*? Рассмотрим несколько точек зрения взятых из юридической литературы.

Под неправомерным доступом к охраняемой законом компьютерной информации, полагает профессор С.В. Бородин, следует понимать самовольное получение информации без разрешения собственника или владельца. В связи с тем, что речь идет об охраняемой законом информации, неправомерность доступа к ней потребителя характеризуется еще и нарушением установленного порядка доступа к этой информации. Если нарушен установленный порядок доступа к охраняемой законом информации, согласие ее собственника или владельца не исключает неправомерности доступа к ней [7]. Немного противоречащее определение, где непонятно почему, ставиться «во главу угла» установленный порядок доступа.

А вот другой взгляд, Т.И. Ваулина считает: «*неправомерным следует признать доступ в закрытую информационную систему лица, не являющегося законным пользователем либо не имеющего разрешения для работы с данной информацией*» [8]. Здесь, как видим, обговаривается два вида доступа: по закону и по разрешению (видимо владельца или собственника). Однако, не понятен объект доступа - *закрытая информационная система*, а не конкретная информация.

Есть еще мнение В. Наумова, который утверждает, что «*неправомерным признается доступ к защищенной компьютерной информации лица, не обладающего правами на получение и работу с данной информацией, либо компьютерной системой*» [9]. Здесь не совсем ясно, в каком смысле информация может быть защищенной – законом или технически? И кто может наделить правами? А ведь мы стремимся к ясности подхода.

Ю. Гульбин считает, что *неправомерным является доступ, противоречащий*

действующим правовым нормам, актам управления, приказам, распоряжениям и иным актам, регуливающим отношения по доступу лиц (группы лиц) к информации[\[10\]](#).

Видится правильным, в рамках данного состава, не применять к *неправомерному доступу* связь с нормативными актами (так сказать, не ставить как антипод законному использованию информации). Иначе будет непонятно как воспринимать несанкционированный владельцем доступ к информации, порядок доступ к которой не урегулирован нормами права. Также, диспозиция статьи 272 УК РФ будет, в этом случае, выглядеть непоследовательной.

С нашей точки зрения, правильным будет избрать подход, основанный на выведенном ранее понятии доступа, который очень точно выразил **В.В. Крылов**:

под неправомерным доступом к компьютерной информации следует понимать не санкционированное собственником информации ознакомление лица с данными, содержащимися на машинных носителях или в ЭВМ[\[11\]](#).

Однако, остается один нерешенный вопрос: о необходимости защиты информации собственником. Другими словами для признания доступа *неправомерным* требуется ли, чтобы для этого были преодолены некоторые преграды или можно будет говорить о неправомерности даже тогда, когда информация находится на общедоступном компьютере (например, в универсамах устанавливаются такие для поиска справочной информации) без средств защиты или предупреждения.

Если обратиться к Закону о информации, то мы увидим, что позиция законодателя по данному вопросу разъясняется в ст. 22:

Собственник документов ... или уполномоченные им лица ... устанавливают порядок предоставления пользователю информации ... А владелец ... обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.

Следовательно, информация должна быть защищена и тогда наше определение «неправомерного доступа» будет выглядеть следующим образом:

под неправомерным доступом к компьютерной информации следует понимать не санкционированное собственником или владельцем информации ознакомление лица с данными, содержащимися на машинных носителях или в ЭВМ, и имеющих уровень защиты в соответствии с законодательством Российской Федерации.

В данном случае показателен следующий пример из судебной практики:

Уголовное дело № 010317 возбуждено 6 февраля 1999 года г. Вологда. Из обвинительного заключения следует, что Ченцов продолжительное время работавший в ООО «Фирма Самогон», в 1998 году вступил в предварительный сговор с Захаровым, направленный на хищение ликероводочной продукции в крупных размерах.

Ченцов – являлся главным специалистом по осуществлению сбыта и маркетинга в регионах путем организации представительств фирмы и контроля за их деятельностью. Прав пользования компьютером и доступа в компьютерную базу головного предприятия не имел. Однако, используя служебное положение, он занимал временно свободные рабочие места, оснащенные включенным компьютером в помещении службы сбыта фирмы. Используя возможность свободного доступа к ЭВМ, умышленно нарушил права владельца компьютерной информации, охраняемые Законом Об информации и другими законодательными актами, осуществил неправомерный доступ к сети ЭВМ ООО «Фирма Самогон» при следующих обстоятельствах:

28 декабря 1998 года в 13 часов 30 минут он, находясь в помещении службы сбыта, с помощью компьютера «Пентиум 120», проник в локально-вычислительную сеть ЭВМ ООО «Фирма Самогон» где:

- уничтожил в списке клиентов фирмы запись «281» – номер договора с Коношским хлебокомбинатом от 05.02.1998 г.;
- модифицировал информацию ЭВМ путем создания заведомо ложной записи в реестре клиентов фирмы, что явилось основанием для отгрузки продукции, которая была похищена, а фирме причинен ущерб в крупном размере.

Своими умышленными действиями Ченцов А.М. совершил неправомерный доступ к охраняемой законом компьютерной информации в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети и это деяние повлекло уничтожение и модификацию информации, совершенное лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети т.е. преступление, предусмотренное ст. 272 ч. 2 УК РФ [\[12\]](#).

Итак, следователь утверждает, что Ченцов совершил «неправомерный доступ», причем путем проникновения в локально-вычислительную сеть, где уничтожил и модифицировал информацию. Ситуация по меньшей мере непонятная, для чего в ней следует разобраться. Если рассматривать ее с технической стороны, то компьютерная информация не может находиться в локально-вычислительной сети, а лишь передаваться с ее помощью, хотя возможно ее изменение в процессе передачи с одного компьютера на другой, но при наличии трех элементов: 1) наличие третьего компьютера находящегося в этой же сети; 2) сложного программного обеспечения; 3) и высокую квалификацию злоумышленника. В остальных случаях для манипуляции с компьютерной информацией – она должна находиться на машинных носителях или ЭВМ. Следовательно, утверждать, что кто-либо проник в сеть и уничтожил «в списке клиентов фирмы запись «281» - не корректно.

Правда, в обвинительном заключении имеется информация проясняющая ситуацию, например свидетельские показания:

Свидетель Мехаленко – ведущий специалист отдела программирования фирмы «Самогон» показал: «На предприятии развернута локально-вычислительная сеть (ЛВС) на 50 рабочих мест с одним сервером под управлением операционной системы Novell 3.12». «В сети на компьютерах установлены и используются пакет бухгалтерских программ «Бухгалтерия 1с 2.0 проф», правовая многопользовательская версия системы «Консультант+», программа по ведению учетных карточек клиентов «Счет 62.1», также программа взаимодействующая с «Счет 62.1» – «Счет 64.2» – программа для учета оборота возвратной тары, комплекс программ по учету отгрузки готовой продукции «RE». «Программа «Счет 62.1» фиксирует поступление средств от клиента и отгрузку продукции. При помощи меню осуществляется обращение к различным режимам: просмотр текущего сальдо клиента, история платежей и отгрузки (карточка по счету), карточка клиента (справочник организаций). Каждый компьютер, подключенный к ЛВС условно закреплен за соответствующим работником определенного отдела. Компьютерная сеть находится в работающем состоянии с 7 часов утра до 19 часов каждый день, кроме субботы и воскресенья. Компьютеры находятся в служебных кабинетах. Кабинеты средствами защиты, охранной сигнализации в основном не оснащены. Сигнализацией оснащены только 2 кабинета: посудный цех и касса». «В подразделениях, связанных с процессом отгрузки продукции и на рабочем месте юриста Смирновой доступ к операционной системе и ЛВС осуществляется через пароль, уникальный для данных рабочих мест и вводимый при включении компьютера, а также при вхождении в ЛВС. Другими словами, для доступа к работе в ЛВС, необходимо ввести 2 пароля. По опыту работы я знаю, что эти пароли одинаковы на определенном рабочем месте. Пароли для входа в ЛВС не менялись с

середины 1998 года, со времени установки сети». «Специальной защиты компьютерной информации или файлов с данными для пользователя, обладающего элементарными навыками работы с популярным комплексом программ «Norton Commander» в ЛВС ООО «Фирма Самогон» не существует. Существующая защита в виде паролей носит условный характер и может помешать лишь постороннему человеку, попавшему на рабочее место». «Информация, содержащая данные реквизитов клиентов предприятия находится в файле по адресу: K:\ORG\parorg.dbf на сервере. Штатным образом изменение реквизитов клиента (добавка новых, удаление старых) осуществляется через соответствующие пункты меню «Работа со справочником организаций». Внесение изменений возможно с любого рабочего места, оснащенного ЛВС, за исключением изменения реквизитов: номера договора и даты договора, доступ на изменение которых осуществляется только определенными пользователями. Существует понятие «типа пользователя». В зависимости от типа пользователя существует возможность внесения изменений в реквизиты карточки клиента. Существуют «главный», «второстепенный», «третий», «четвертый» типы пользователей при работе в программе «Счет 62.1». Приоритет на внесение изменений в карточку пользователя, в части изменения номера договора и его даты, условия оплаты за продукцию принадлежит только «четвертому» типу пользователя. Такой тип пользователя установлен на компьютерах находящихся на рабочих местах юриста Смирновой И.А., инженера Поляковой В.А. и на рабочем месте программиста Ляпина А.Ю. [13].

Данные программистом показания дают исчерпывающие сведения о технической стороне работы локально-вычислительной сети и процесса использования компьютерной информации. Из них можно заключить, что Ченцову для осуществления неправомерного доступа и модифицирования информации требовалось преодолеть защиту из двух паролей (для этого их нужно было знать изначально или получить несанкционированным путем) и изменить файл K:\ORG\parorg.dbf на сервере, но об этом ничего не говорится в выводах следователя. Хотя защиту нельзя признать серьезной и, как выясняется из следующих показаний, в некоторых случаях, ее можно считать отсутствующей:

Свидетель Смирнова – юристконсульт отдела сбыта фирмы «Самогон» показала, что никакого пароля на доступ во время работы к ее компьютеру, программе «Счет 62/1» и компьютерной сети не было, потому данные мог ввести любой человек, оказавшийся в кабинете в ее отсутствие» [14].

Здесь Смирнова имеет в виду, что когда компьютер запущен и загружена программа «Счет 62.1», в ее отсутствие для осуществления манипуляций с данными программы не требуется никакого пароля. Окончательные детали неправомерного доступа можно почерпнуть из показаний самого Ченцова:

Допрошенный в качестве обвиняемого Ченцов показал, 28 декабря 1998 года, в обеденный перерыв, сел за компьютер инженера службы сбыта и маркетинга Поляковой, который был подключен к компьютерной сети, компьютер был включен, на экране была страница из реестра клиентов фирмы «Самогон». Создал в реестре новую учетную карточку клиента, которую заполнил реквизитами ООО «Предприятие». Для сохранения записи нажал клавишу «Pg Dn». «Вечером 28 декабря я встретился с Захаровым и сказал, что все данные в компьютер введены и можно вывозить продукцию. Также я дал ему подробные инструкции, как нужно оформить документы при получении продукции на «Самогоне» [15].

Итак, неправомерный доступ выглядел следующим образом:

Ченцов, находясь в кабинете, где имел право находиться в силу своей должности, с помощью компьютера, использовать который он права не имел, и без преодоления защиты изменил в уже запущенной программе информацию, на изменение которой у

него права не было.

Можно ли назвать действия Ченцова – неправомерным доступом? Видимо – да! Так как выполнены все четыре условия неправомерного доступа:

1. данные находились в ЭВМ;
2. для доступа к ним был установлен уровень защиты, хотя и «слабый», но Ченцов знал, что информация защищена паролями и от него тоже;
3. перед модификацией Ченцов ознакомился с данными;
4. ознакомление было несанкционированным, т.к. политика ООО «Фирма Самогон» по использованию информации коммерческого характера содержащейся на ЭВМ подразумевала возможность ознакомления и изменения ее строго определенными сотрудниками, в число которых Ченцов на тот момент не входил.

Другим примером «неправомерного доступа» является уголовное дело из г. Екатеринбург:

Главным Следственным Управлением ГУВД по Свердловской области совместно с Управлением «Р» возбуждено уголовное дело по ст. 272 за «неправомерный доступ к анонимному (*для работы не требовалась авторизация*) прокси-серверу, что повлекло причинение материального ущерба компании владельцу сервера (оплата трафика)».

За неимением большей информации проанализируем данную формулировку. Назвать это **неправомерным доступом** никак **нельзя** потому, что:

1. прокси-сервер – это не данные, а программа и в рамках сети Интернет является публичным сервисом;
2. авторизации не было, т.е. не было никакого пароля или иного уровня защиты;
3. ознакомления не было, т.к. не было данных;
4. и несанкционированными данные действия назвать нельзя, т.к. прокси-сервер был выставлен свободно в сети Интернет.

А о последствиях в виде материального ущерба нет смысла и говорить в рамках ст. 272 УК РФ. Потерпевшей стороне нужно было не «в милицию бежать», а обращаться к юристам и составлять заявление на гражданский иск.

[1] Андреев б.В., Пак П.Н., Хорст В.П. *Расследование преступлений в сфере компьютерной информации*. М.: ООО Изд. «Юрлитинформ», 2001. С. 37.

[2] Там же.

[3] *Комментарий к Уголовному кодексу Российской Федерации* / Под ред. Ю. И. Скуратова и В. М. Лебедева. – М.: Издательская группа ИНФРА*М – НОРМА, 2001. С.698.

[4] Обвинительное заключение по уголовному делу № 011678 // http://kurgan.unets.ru/~procur/my_page.htm

[5] Строка на Интернет-странице, позволяющая при нажатии переходить на другую страницу.

[6] [LENTA.RU В суд за ссылку: новгородская версия // Материалы Интернет-страницы: http://lenta.ru/internet/2000/02/03/porno/_Printed.htm](http://lenta.ru/internet/2000/02/03/porno/_Printed.htm)

[7] *Комментарий к Уголовному кодексу РФ*/ Отв. ред. **А.В. Наумов**. С. 663.

[8] *Уголовное право. Особенная часть*//Отв. ред.: **И.Я. Козаченко, З.А. Незнамова, Г.П. Новоселов**- М.: Изд. НОРМА-Инфра*М. 1998. С.557.

[9] **В. Наумов** *Отечественное законодательство в борьбе с компьютерными преступлениями* // <http://www.hackzone.ru/articles/a5.html>

[10] **Гульбин Ю.** *Преступления в сфере компьютерной информации* // "Российская юстиция". 1997. № 10

[11] **Крылов В.В.** Указ. соч. С. 40.

[12] Обвинительное заключение по уголовному делу № 010317 // http://kurgan.unets.ru/~procur/my_page.htm

[13] Обвинительное заключение по уголовному делу № 010317 // http://kurgan.unets.ru/~procur/my_page.htm

[14] Обвинительное заключение по уголовному делу № 010317 // http://kurgan.unets.ru/~procur/my_page.htm

[15] Обвинительное заключение по уголовному делу № 010317 // http://kurgan.unets.ru/~procur/my_page.htm

§ 2. Охраняемая законом компьютерная информация

Следующим вопросом в диспозиции статьи 272 УК РФ стоит *охраняемая законом компьютерная информация* – предмет данного преступления. Как пояснили С.В. Бородин и С.В. Полубинская: *непосредственным объектом данного преступления является безопасность использования компьютерной информации, информационных ресурсов и систем. А предметом преступления будет компьютерная (машинная) информация, содержащаяся на машинном носителе, в ЭВМ, их системе или сети, охраняемая законом, т.е. изъятая из открытого оборота на основании закона, иного нормативного правового акта, а также правил внутреннего распорядка, основанных на названных правовых актах*[1]. Под охраняемую подпадает:

- информация, составляющую государственную тайну, режим защиты которой устанавливается федеральным законом;
- конфиденциальная информация, режим защиты устанавливается в основном собственником или владельцем на основании закона, а в ряде случаев федеральным законом;
- документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Режим защиты устанавливается собственником или владельцем на основании закона.

Есть мнение среди юристов-теоретиков, что «под охраняемой законом информацией понимается документированная информация, для которой установлен специальный режим правовой защиты»[2], т.е. вся информация, и содержащая государственную тайну, и конфиденциальная информация, находящаяся в ЭВМ, чтобы стать охраняемой законом, должна быть документирована. Но придание информации статуса охраняемой законом в

зависимости от формы представления, а не от содержания, **нельзя признать верным**. Государственная тайна остается государственной тайной, даже если на электронном документе, содержащем ее, нет электронной цифровой подписи.

Компьютерная информация может быть представлена в форме информационных ресурсов, которые в ст.2 Закона об информации рассматриваются как отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах, в частности в банках данных. Эти ресурсы согласно ст. 2 Закона содержат сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [3], где банки (или базы) данных являются объективной формой представления и организации совокупности данных, систематизированных таким образом, чтобы они могли быть найдены и обработаны с помощью ЭВМ[4].

Рассмотрим как на практике применяется законодательство об охраняемой информации. Например, в уголовном деле Ченцова рассмотренном выше, имеется такая точка зрения, взятая следователем из заключения эксперта по программно-технической экспертизе от 27 мая 1999 года и состоит в том, что «база данных, находящаяся в ЛВС ООО «Фирма Самогон» является компьютерной информацией и потому охраняется действующим федеральным законом «Об информации, информатизации и защите информации» [5]. Не совсем ясно, почему юридическую оценку предмету преступления дает эксперт, что само по себе является нарушением уголовно-процессуального закона, но еще более сомнительной является логика о том, что информация является охраняемой законом в силу того, что она компьютерная.

На практике часто встречаются уголовные дела, возбужденные по факту незаконного копирования и использования идентификационных данных[6] для доступа в Интернет, под которыми обычно подразумеваются регистрационное имя и пароль абонента. Рассмотрим некоторые из них.

Уголовное дело №444800 возбужденное 29.02.2000 года в г. Шадринске. Из обвинительного заключения по уголовному делу установлено, что Полетаев, работая в должности инженера-программиста на Шадринском телефонном заводе, на компьютере Pentium, процессор Intel MMX, подключенном с помощью модема к телефонной линии, имея умысел на неправомерный доступ к компьютерной информации, охраняемой в установленном законом порядке и принадлежащей Шадринскому Региональному Управлению Федеральной Почтовой Связи, из корыстных побуждений, желая подключиться к сети Интернет за счет Шадринского РУФПС, в декабре 1999 года скопировал из Интернета программу типа «троянский конь» – имитирующую нормальную работу ЭВМ и одновременно негласно для пользователя предоставляющую полный доступ к компьютеру. Эту программу Полетаев направил в виде текстового документа на электронный адрес Шадринского РУФПС. Когда пользователь на компьютере РУФПС открыл данный документ, сработала программа «троянский конь», при работе которой пользователь РУФПС не подозревал о ее существовании, а программа предоставляла Полетаеву возможность просматривать и копировать на свой компьютер всю информацию имеющуюся на компьютере РУФПС. Полетаев, во время подключения компьютера РУФПС к сети Интернет, зашел на его жесткий диск с целью скопировать два файла с паролями Шадринского РУФПС, и просмотрев его содержимое скопировал из каталога C:\WINDOWS два файла: – user.dat и имя.pwl, на свой компьютер, принадлежащий конструкторскому бюро Шадринского телефонного завода.

Таким образом, своими умышленными действиями Полетаев совершил преступление, предусмотренное ст. 272 ч. 2 УК РФ – НЕПРАВОМЕРНЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ – то есть информации на машинном носителе, в электронно-

вычислительной машине (ЭВМ), системе ЭВМ или их сети, повлекший копирование информации, совершенный лицом с использованием своего служебного положения [7].

Данное уголовное дело – это классический пример. 3-4 года назад примерно 1/5 компьютерщиков разной квалификации именно приведенным способом «добывала» себе бесплатный доступ в Интернет. Таким же способом похищены и использованы файлы пользователей в уголовном деле № 30, переданном в суд следователем РУ ФСБ РФ по Архангельской области по обвинению Гренц А.А. Петрова И.В. в совершении преступлений, предусмотренных ч.2 ст. 272 УК РФ [8].

Сейчас мы имеем возможность, взглянуть на данную проблему с юридической точки зрения. В описанном примере судебной практики реализован один из технически «чистых» случаев *неправомерного доступа к информации*. Не вдаваясь в технические детали, рассмотрим юридические: Полетаев, получил доступ и имел возможность ознакомиться с любыми данными, находящимися на компьютере Шадринского РУФПС, где существовал уровень защиты, обусловленный уровнем защиты операционной системы от внешнего вторжения, а доступ Полетаева был несанкционированный, т.к. собственник о нем ничего не знал. Можно сказать, что и с юридической стороны первоначальные действия Полетаева нужно назвать **неправомерным доступом**. Но можно ли назвать скопированные им файлы user.dat и имя.pwl – *охраняемой законом компьютерной информацией*? Посмотрим еще на один пример:

Уголовное дело № 9010076 возбужденное 23 июня 1999 г. по ст.158 ч.3 п. "б" УК РФ в отношении Мальцева и Нефедова, в дальнейшем перекалфицировано на ст. ст. 272 ч.2, 183 ч.1, ч.2 УК РФ.

Согласно обвинительному заключению: Мальцев, работая начальником автоматизированной системы управления ЗАО "Расчетно-Маркетинговый Центр" г.Уфы (далее ЗАО «РМЦ»), в декабре 1998 г. вступил в преступный сговор с программистом ЗАО «РМЦ» Нефедовым. Используя свое служебное положение, обладая достаточными знаниями в области пользования компьютерной техники и опытом работы в глобальной сети Интернет, Мальцев через сеть Интернет, в период времени с декабря 1998 г. по июнь 1999 г. получил доступ к другим ЭВМ, принадлежащим Управлению производственно-жилищного хозяйства и инженерного обеспечения Администрации г. Уфы (далее УПЖХИО), ООО "Клиринг" г. Уфы и Центру "РИД". Заведомо зная, что пароли к сети Интернет хранятся в файлах «rwl» и зашифрованы методом "DES", и зная о наличии программ - "смотрелок", предназначенных для декодировки файлов, Мальцев выбрал программу «PWLHACK». С помощью этой программы Мальцев совместно с Нефедовым, умышленно, осуществляли неправомерный доступ к охраняемой законом компьютерной информации ИКЦ "Экспресс" – логинам и паролям для доступа в сеть Интернет, с рабочих компьютеров, установленных в ЗАО "Расчетно-Маркетинговый Центр". Указанные действия были предприняты ими несмотря на то, что они заведомо знали, что их преступные действия повлекли блокирование работы законных абонентов ИКЦ "Экспресс" в сети Интернет, а также нарушение работы сети ЭВМ ИКЦ "Экспресс", и кроме того, копирование охраняемой законом компьютерной информации: выразившееся в переносе информации с одного физического носителя на другой помимо воли собственника, то есть перенос информации на свой персональный компьютер. Собравшие, таким образом, логины и пароли для доступа в сеть Интернет, Мальцев совместно с Нефедовым, из корыстных побуждений и с целью причинения крупного ущерба ИКЦ "Экспресс", использовали как сами, так и разглашали их третьим лицам, без согласия на то законных владельцев. В результате преступных деяний Мальцева и Нефедова, за период времени с декабря 1998 г. по июнь 1999 г. ИКЦ "Экспресс" был причинен материальный ущерб на общую сумму 16 174 рубля 33 копейки, являющийся крупным для данного

предприятия [9].

Как видно из данного уголовного дела именно «пароли к сети Интернет хранятся в файлах «pwl» и зашифрованы методом "DES"», а если быть более точными в файлах user.dat и имя.pwl операционная система Microsoft Windows 95 (а также Windows 98) хранит идентификационные данные, получаемые при заполнении форм доступа к глобальной сети Интернет. То есть файлы user.dat и имя.pwl являются частью операционной системы, являются ее служебными файлами, а операционная система, как известно, является программным обеспечением, а программное обеспечение, в свою очередь, не является охраняемой законом компьютерной информацией. Хотя, например, следователь из рассматриваемого ранее уголовного дела № 011678 по обвинению Федорова считает, что программы нужно считать охраняемой законом компьютерной информацией, аргументируя это тем, что:

согласно статье 3 Федерального Закона «О правовой охране программ для электронных вычислительных машин и баз данных», предоставляемая настоящим Законом правовая охрана распространяется на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код. Предоставляемая настоящим Законом правовая охрана распространяется на базы данных, представляющие собой результат творческого труда по подбору и организации данных. Базы данных охраняются независимо от того, являются ли данные, на которых они основаны или которые они включают, объектами авторского права.

И он совершенно прав, что программам, как объектам авторского права, предоставляется правовая охрана, как произведениям литературы. Но в данном случае, охраняется не сама информация, заложенная в программы, а авторские права по использованию и распространению программ и баз данных. А как сказано, в п. 2 ст. 1 Закона об информации, устанавливающего защиту компьютерной информации:

Настоящий Федеральный закон не затрагивает отношений, регулируемых Законом Российской Федерации "Об авторском праве и смежных правах".

Итак, программное обеспечение не является охраняемой законом компьютерной информацией, т.е. копирование файлов операционной системы, даже после неправомерного доступа, выходит за рамки ст. 272 УК РФ.

Но интересующие нас файлы user.dat и имя.pwl не просто служебные файлы операционной системы, а файлы, содержащие идентификационные данные абонента доступа к глобальной сети Интернет и представляют собой регистрационное имя и пароль (а в некоторых случаях адрес шлюза, прокси-сервера, DNS и статический IP-адрес). Именно эти данные многие на практике считают охраняемой законом компьютерной информацией. Как и перед этим возьмем в качестве цитаты мысль из обвинительного заключения уголовного дела № 011678, хотя такие обоснования есть и в других уголовных делах данной категории:

К охраняемой Законом компьютерной информации в данном случае относятся: информация об имени пользователя и пароле доступа для работы в сети «Интернет», предоставленная Борисову ОАО «Новгородтелеком» согласно договору № 570603 от 7 июля 1999 года и являющейся конфиденциальной согласно пункта 6. 1 данного договора, а также согласно пункта 5 «Перечня сведений конфиденциального характера»,

утвержденного Указом Президента РФ от 6 марта 1997 года № 188 и согласно содержания статьи 139 ГК РФ.

Итак, следователь считает, что идентификационные данные являются конфиденциальной информацией, а точнее коммерческой тайной, в силу чего подпадают под охраняемую законом компьютерную информацию. Но для того, чтобы информацию отнести к коммерческой тайне, нужно, чтобы она отвечала следующим требованиям:

1. имела действительную (или хотя бы потенциальную) коммерческую ценность, т.е. чтобы она давала потребителю возможность использовать ее в целях получения прибыли;
2. была недоступна, т.е. к ней не было бы свободного доступа на законном основании;
3. и охранялась ее обладателем [\[10\]](#).

Здесь мы подходим к одной очень важной проблеме, касающейся природы идентификационных данных. Дело в том, что сами они представляют лишь набор слов, а чаще всего набор букв, и не представляют ни действительной, ни потенциальной коммерческой ценности, а также иной ценности. С другой стороны, эти данные, при определенной деятельности со стороны провайдера, предоставляющего доступ к глобальной сети Интернет, могут стать ключом к доступу. Предоставление доступа к сети Интернет является оказанием возмездной информационной услуги, урегулированным в гл. 39 ГК РФ. А специфика данной услуги заключается в том, что через ее осуществление, т.е. через доступ в Интернет, возможно получить прибыль. Значит, идентификационные данные – лишь первое звено в цепочке получения прибыли через Интернет. Наверное, только в силу данной цепочки (при условии действительной охраны обладателем и недоступности) такие данные можно считать коммерческой тайной, а значит отнести к охраняемой законом информации.

Следовательно, файлы `user.dat` и `имя.pwl` операционной системы Windows, не относятся к охраняемой законом компьютерной информации, но могут в ряде случаев содержать информацию конфиденциального характера. И к какой тогда категории отнести эти файлы? Компания разработчик Microsoft постаралась сделать их именно частью своего программного обеспечения, зашифровав конфиденциальную информацию с помощью криптографического алгоритма «DES» и раскидав ее по разным файлам, что не подразумевало непосредственного несанкционированного доступа к ней. И если бы информация оставалась в таком недоступном виде, то указанные файлы не могли бы претендовать на защиту закона. Однако, пытливые хакеры и кракеры нашли и научились расшифровывать такую информацию, т.е. конфиденциальную информацию стало возможно представить в понятном для человека виде с помощью специальных утилит. А если придерживаться точки зрения, когда конфиденциальная информация остается таковой вне зависимости от формы, в которой она сохранена, то файлы операционной системы, где сохранены идентификационные данные, нужно считать конфиденциальной информацией и относить к охраняемой законом компьютерной информации.

На основании данных выводов можно утверждать, что в обоих вышеприведенных случаях, как в уголовном деле Полетаева, так и в уголовном деле Мальцева и Нефедова, осуществлен неправомерный доступ именно к охраняемой законом компьютерной информации.

- [1] *Уголовное право России. Особенная часть.* / Под ред. **В.Н. Кудрявцева, А.В. Наумова.** – М.: Юристъ, 2000. С.349.
- [2] **Панфилова Е.И., Попов А.Н.** Указ. соч. с. 28.
- [3] *Комментарий к Уголовному кодексу РФ.* / Отв. ред. **А.В. Наумов.** С. 662.
- [4] Закон РФ «О правовой охране программ для ЭВМ и баз данных» от 23.09.92 №3526-1 // Российская газета, № 230. 21.10.92.
- [5] Обвинительное заключение по уголовному делу № 010317 // http://kurgan.unets.ru/~procur/my_page.htm
- [6] Смысл термина «идентификационные данные» в данном случае взят из компьютерной терминологии и отличен от терминологии, принятой в криминалистике.
- [7] Обвинительное заключение по уголовному делу № 444800 // http://kurgan.unets.ru/~procur/my_page.htm
- [8] Обвинительное заключение по уголовному делу № 30 // http://kurgan.unets.ru/~procur/my_page.htm
- [9] Обвинительное заключение по уголовному делу № 9010076 // http://kurgan.unets.ru/~procur/my_page.htm
- [10] Постатейный комментарий к части первой ГК РФ/ **Гуев А.Н.** – М.: Инфра*М, 2000. С.270.

3. Информации на машинном носителе, в ЭВМ, системе ЭВМ, сети

Вернемся к диспозиции статьи 272, где говорится о *неправомерном доступе к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети*, и рассмотрим в некоторых деталях определенные законодателем места нахождения информации.

К машинным носителям, которые позволяют хранить информацию, относятся гибкие диски (дискеты), компакт-диски и оптические диски. Несколько лет назад и в некоторых случаях и сейчас под машинными носителями информации использовали всякого рода магнитные диски, магнитные ленты, магнитные барабаны, перфокарты, полупроводниковые схемы и др. Некоторые считают, что жесткие диски нужно считать машинными носителями информации. С технической точки зрения это правильно и на них возможно хранение информации, но дело в том, что жесткие диски являются конструктивной частью компьютера, без которой вряд ли можно представить сегодня современные компьютеры, и поэтому когда жесткий диск установлен в компьютере, информация, сохраненная на нем, считается находящейся *в электронно-вычислительной машине*. И только, когда жесткий диск конструктивно отделен от компьютера, его можно считать машинным носителем информации.

Законодательная конструкция «информации в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети» очерчивает лишь рамки нахождения информации. Хотя в ЭВМ, например, информация, может находиться как на жестком диске, так в оперативной памяти, а разница между модификацией информации в этих местах принципиальна. Законодатель ограничился только фактом, что информация может находиться в ЭВМ (или системе, сети) и неважно в какой форме, что вполне оправдано, т.к. для компьютерной информации нет принципиального значения, где находится, она в

любом случае нуждается в защите. С технической точки зрения отличие информации на данной ЭВМ от информации на удаленной ЭВМ, обращение к которой осуществляется по компьютерной сети, заключается только в способах и методах доступа к ней.

§ 4. Обязательные последствия

Состав преступления статьи 272 УК РФ сформулирован как материальный, причем если деяние в форме действия определено однозначно (неправомерный доступ к охраняемой законом компьютерной информации), то последствия, хотя и обязательны, могут быть весьма разнообразны: 1) уничтожение информации, 2) ее блокирование, 3) модификация, 4) копирование, 5) нарушение работы ЭВМ, 6) то же — для системы ЭВМ, 7) то же — для их сети.

Мнение, что для наступления уголовной ответственности *неправомерный доступ к охраняемой законом компьютерной информации должен повлечь одно из последствий* [1], является основным среди юристов-теоретиков. Однако, как правильно отметил Г.П. Новоселов, именно термин «повлекло» дает основание полагать, что объективная сторона данного состава преступления складывается из деяния (неправомерного доступа), последствий (уничтожение информации и т.д.) и причинной связи между ними. Но нельзя не признать, что уничтожение, блокирование, модификация и копирование информации не исключают совершения самостоятельных действий. Представляется, что правильнее было бы рассматривать основанием уголовной ответственности за неправомерный доступ к компьютерной информации случаи, когда неправомерный доступ сопряжен с уничтожением, блокированием и т.д. (т.е. такому доступу следовало бы придать значение не только причины, но и необходимого условия) [2].

Считаем нужным согласиться с данным мнением потому, что, с технической стороны, из всех последствий только нарушение работы ЭВМ, системы ЭВМ или их сети можно назвать *последствием* в полном смысле этого слова. Остальные последствия перечисленные в диспозиции будут таковыми только в **некоторых**, точнее в **редких**, случаях. В основном для того, чтобы информацию уничтожить, заблокировать, копировать, модифицировать, а также нарушить работу ЭВМ, системы ЭВМ или сети, **требуется выполнить самостоятельное действие, а чаще ряд действий.**

Например, в описанном выше уголовном деле № 444800 [3] была такая последовательность действий:

в декабре 1999 года Полетаев скопировал из Интернета программу типа «троянский конь». Эту программу он направил в виде текстового документа на электронный адрес Шадринского РУФПС. Когда пользователь на компьютере РУФПС открыл данный документ, сработала программа, при работе которой пользователь РУФПС не подозревал о ее существовании, а программа предоставляла Полетаеву возможность просматривать и копировать на свой компьютер всю информацию, имеющуюся на компьютере РУФПС. Полетаев, во время подключения компьютера РУФПС к сети Интернет, **зашел** на его жесткий диск и **просмотрел** его содержимое -

тем самым, выполнив **неправомерный доступ к информации**, а после чего отдельными действиями -

скопировал из каталога C:\WINDOWS два файла: – user.dat и имя.pwl, на свой компьютер.

Поэтому, будет правильным принять формулировку **Е.И. Панфиловой и А.Н. Попова**

А.Н., которые считают, что *объективная сторона преступления, предусмотренного ст. 272 УК РФ, выражается в двух действиях:*

· **неправомерный доступ** к компьютерной информации, находящейся в ЭВМ, системе ЭВМ, сети ЭВМ или на машинном носителе;

· **второе действие** ...альтернативно – или уничтожение, или блокирование, или модификация либо копирование информации [4].

К этому нужно добавить, что *вторым действием может* выступать и самостоятельное действие направленное на возникновение нарушения работы ЭВМ, системы ЭВМ или их сети, **но** чаще всего *нарушение работы* является последствием одного из двух вышеперечисленных действий.

Следует остановиться еще на одном аспекте – причинной связи. Как отмечают в юридической литературе, *немаловажным является установление причинной связи между несанкционированным доступом и наступлением вредных последствий. При функционировании сложных компьютерных систем возможны уничтожение, блокирование и иные нарушения работы ЭВМ в результате технических неисправностей или ошибок в программных средствах*[5], т.е. простое временное совпадение момента сбоя в компьютерной системе, которое может быть вызвано неисправностями или программными ошибками, и неправомерного доступа не влечет уголовной ответственности[6].

Именно факт установления причинной связи приводит правоприменителя в замешательство. Ввиду того, что неправомерный доступ в основном является условием для осуществления непосредственно второго действия (например, копирования), то их сложно связать с помощью причинной связи. В связи с этим, в обвинительных заключениях встречаются некорректные, с технической точки зрения, формулировки о причинной связи между неправомерным доступом и последствиями, но чаще следователи не устанавливают ее, а упоминают о ней, указывая лишь на общую последовательность отдельных действий, как в уголовном деле Полетаева. Есть даже примеры, где следователи, пытаясь показать причинную связь, «нагромождают» лишними, выходящими за рамки статьи 272, последствиями. Для примера, можно еще раз взглянуть на описанное ранее уголовное дело[7] Мальцева и Нефедова, где они:

осуществляли неправомерный доступ к охраняемой законом компьютерной информации ИКЦ "Экспресс" - логинам и паролям для доступа в сеть Интернет. Их преступные действия **повлекли блокирование работы** законных абонентов ИКЦ "Экспресс" в сети "Интернет", выражающееся в том, что при входе в сеть Интернет одного пользователя, под определенным логином и паролем, доступ в Интернет правомочных пользователей под аналогичным логином и паролем исключен, а также **нарушение работы сети ЭВМ** ИКЦ "Экспресс", выражающейся в том, что ограничивается работа легальных пользователей, так как происходит непредусмотренная нагрузка на связанное оборудование: наличие дополнительного трафика ведет к уменьшению скорости передачи и обработки информации, а повышенная загрузка оборудования приводит к увеличению ошибок при передаче данных, и как следствие, к искажению принимаемой или отправляемой информации, использование нестандартных приемов работы с сетевыми ресурсами приводит к блокированию работы сетевого оборудования, и **кроме того**, копирование охраняемой законом компьютерной информации: выразившееся в переносе информации с

одного физического носителя на другой помимо воли собственника, то есть перенос информации на свой персональный компьютер[8].

Здесь следователь совершенно необоснованно указал на последствия в виде *блокирования работы и нарушения работы сети ЭВМ*, и некорректно связал копирование информации, как следствие, с неправомерным доступом к логинам и паролям.

Из-за общей некомпетентности всех правоохранительных органов, и суда в частности, в компьютерных вопросах, на такие факты мало кто обращает внимание, а между тем, это нарушение уголовного и уголовно-процессуального законодательства.

Рассмотрим действия второго плана, с которыми уголовный закон связывает наступление уголовной ответственности:

Уничтожение информации — наиболее опасное явление, поскольку при этом собственнику информации наносится максимальный реальный вред.

Несмотря на достаточно широкое в целом использование термина «уничтожение» в общеупотребительной лексике, в юридической литературе уже наметились тенденции, связанные с различиями в трактовке термина «уничтожение информации», введенного законодателем в УК РФ.

Так, некоторые ученые считают, что *уничтожение информации представляет собой ее удаление с физических носителей*[9], а также *несанкционированные изменения составляющих ее данных, кардинально меняющие ее содержание (например, внесение ложной информации, добавление, изменение, удаление записей)*[10].

Другие полагают, что под *уничтожением информации следует понимать ее утрату при невозможности ее восстановления*[11] или *стирание ее в памяти ЭВМ*[12].

Наконец, ряд специалистов рассматривают уничтожение информации как *приведение ее либо полностью, либо в существенной части в непригодное для использования по назначению состояние*[13]. Или же, как *полную физическую ликвидацию информации или ликвидацию таких ее элементов, которые влияют на изменение существенных идентифицирующих признаков*[14].

Однако, говорить о *полной физической ликвидации информации* чаще всего некорректно. Дело в том, что операционные системы редко когда удаляют информацию, даже если это проделал непосредственно пользователь. Например, операционная система «MS DOS v6.22» при удалении файла с информацией не удаляет его, а лишь изменяет имя файла и переносит в скрытый список и только с течением времени, если информация осталась не востребованной, она действительно уничтожает ее, записывая на ее место другую. Или другой пример, общеизвестно, что форматирование машинного носителя информации, будь то жесткий диск или дискета, полностью уничтожает всю информацию на носителе, но технически это не соответствует действительности и с помощью специализированных утилит информацию возможно восстановить. Итак, мы приходим к выводу, что рядовой пользователь, удалив информацию, считает ее удаленной и действительно не имеет возможности ее использовать, но для специалиста не составляет труда восстановить информацию, часто без искажения.

Ввиду того, что на данный момент очень сложно отграничить рядового пользователя от специалиста, потому что таким может стать и человек без специального образования. Представляется, что будет правильным считать под «уничтожением информации» -

удаление информации с носителя без технической возможности восстановления.

Модификация информации. Вопрос о модификации информации является весьма сложным. В специализированных словарях термин «модификация» используют для обозначения изменений, не меняющих сущности объекта. Подобные действия над компьютерной информацией напрямую связаны с понятиями «адаптации» и «декомпиляции» программ, уже существующими в действующем законодательстве.

Например, статьей 15 Закона о правовой охране программ установлено, что лицо, правомерно владеющее экземпляром программы для ЭВМ или базы данных, вправе без получения дополнительного разрешения правообладателя осуществлять любые действия, связанные с функционированием программы для ЭВМ или базы данных в соответствии с ее назначением, в том числе запись и хранение в памяти ЭВМ, а также исправление явных ошибок. Такое лицо вправе без согласия правообладателя и без выплаты ему дополнительного вознаграждения осуществлять адаптацию программы для ЭВМ или базы данных. В других законах установлены подобные положения.

Таким образом, законодательством санкционированы следующие виды легальной модификации программ, баз данных (а следовательно, информации) лицами, правомерно владеющими этой информацией:

- а) модификация в виде исправления явных ошибок;
- б) модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя;
- в) модификация в виде частичной декомпиляции программы для достижения способности к взаимодействию с другими программами.

Рассматривая данную ситуацию, одни юристы полагают, что модификация компьютерной информации — это внесение в нее любых изменений, кроме связанных с адаптацией программы для ЭВМ или базы данных[15]. Другие считают, что под модификацией информации следует понимать внесение в нее любых изменений, обуславливающих ее отличие от той, которую включил в систему и которой владеет собственник информационного ресурса[16]. Третьи рассматривают модификацию информации как изменение логической и физической организации базы данных[17].

Согласимся с С.В. Бородиным, который считает, что ***модификация информации** означает изменение ее содержания по сравнению с той информацией, которая первоначально (до совершения деяния) была в распоряжении собственника или законного пользователя*[18]. Считая, что для квалификации по данной статье не имеет значения, какое изменение и в каком виде информации (в программе или в документе) было сделано, главное установить, что информация охраняется законом и в ней были произведены изменения.

Копирование информации.

Термин «**копирование**» как изготовление копии объекта не требует дополнительных пояснений. Тем не менее, многие юристы, характеризуя это действие, по сути, дают определение частным случаям копирования.

Так, одни полагают, что копирование — это изготовление второго и последующих экземпляров базы данных, файлов в любой материальной форме, а также их запись в память ЭВМ[19]. Другие считают, что копирование компьютерной информации — это

повторение и устойчивое запечатление ее на машинном или ином носителе[20]. Третьи понимают под копированием информации ее переписывание, а также иное тиражирование при сохранении оригинала, а также и ее разглашение[21].

Важным вопросом является проблема мысленного запечатления полученной информации в процессе ознакомления с нею в памяти человека, без которого, кстати, невозможно ее разглашение. Здесь на первый взгляд возникает некий пробел в уголовно-правовой защите конфиденциальности документированной информации, содержащейся в информационных системах[22].

Если придерживаться понимания термина «копирование» только как процесса изготовления копии информации в виде физически осязаемого объекта, то все случаи проникновения злоумышленников в информационные системы, не связанные с копированием (и иными предусмотренными законодателем действиями и (или) последствиями), но приведшие к ознакомлению с информацией независимо от того, какой режим использования информации установил ее собственник, не являются противоправными. По этому поводу, была возмущена «компьютерная общественность» отмечая несправедливость решения, что *простое несанкционированное проникновение в чужую информационную систему без каких-либо неблагоприятных последствий наказанию не подлежит, а неправомерное проникновение в квартиру, дом или офис должно быть наказуемо вне зависимости от последствий деяния*[23].

Многие юристы считают, что *если был неправомерный доступ, не повлекший совершение последующих действий, названных в законе, то ответственность не наступает*[24].

По-видимому, в подобных ситуациях следует рассматривать совершенные лицом действия с учетом существования других уголовно-правовых запретов, касающихся иных форм информационных преступлений (например, статья 183 УК РФ *Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну* и др.)[25].

Способ копирования, на наш взгляд, не имеет существенного значения, поскольку защите в рассматриваемом случае подлежит сама информация, в каком бы месте она не находилась.

В связи с этим нельзя согласиться с высказанным в литературе мнением о том, что копирование компьютерной информации от руки, путем фотографирования с экрана дисплея, а также перехвата излучений ЭВМ и другие подобные способы не охватываются содержанием раздела о преступлениях в области компьютерной информации.

С другой стороны, следует признать справедливым утверждение о том, что нельзя инкриминировать лицу копирование информации в случае, когда в ходе проникновения в ЭВМ и ознакомления с находящейся там информацией программные механизмы ЭВМ автоматически скопируют тот или иной файл[26]. Соглашаясь с этим, **В. В. Крылов** однако, инкриминирует лицу то, что *в ходе ознакомления с чужой информацией злоумышленник на техническом уровне переносит (копирует) информацию в ОЗУ собственной ЭВМ и просматривает ее на экране. Даже если эта информация не распечатывается на бумажные носители — налицо ее копирование с одного машинного носителя на другой машинный носитель*[27]. На наш взгляд, это лишь частный случай первого копирования и производится самостоятельно ЭВМ, что нельзя считать осмысленным копированием.

Итак, **под копированием компьютерной информации** следует понимать изготовление

копии информации в любой материальной форме.

Блокирование информации как термин имеет различные смысловые значения, что и находит свое отражение в его трактовке в литературе.

Некоторые юристы, в частности С.В. Бородин, полагают, что блокирование информации — это невозможность ее использования при сохранности такой информации[28].

Другие указывают, что блокирование компьютерной информации — это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением[29].

Ряд специалистов считают, что блокирование представляет собой создание условий (в том числе и с помощью специальных программ), исключающих пользование компьютерной информацией ее законным владельцем[30].

Некоторые юристы отдельно выделяют аппаратную или программную блокировку ЭВМ, что влечет невозможность использования информации[31].

Полагаем, что **блокирование компьютерной информации** — это совершение действий, результатом которых является временная или постоянная невозможность осуществлять какие-либо операции над компьютерной информацией, при ее сохранности.

Нарушение работы ЭВМ.

В литературе указывается, что нарушение работы ЭВМ, системы ЭВМ или их сети может выразиться в их произвольном отключении, в отказе выдать информацию, в выдаче искаженной информации при сохранении целостности ЭВМ, системы ЭВМ или их сети[32]. Нарушение работы ЭВМ, системы ЭВМ или их сети может рассматриваться и как временное или устойчивое создание помех для их функционирования в соответствии с назначением[33]. Или же, выразиться в снижении работоспособности отдельных звеньев ЭВМ, отключении элементов компьютерной сети[34].

Вышеприведенные точки зрения по большей части некорректны (наиболее явные места подчеркнуты - *нами*) и авторы слабо представляют как работу, так и нарушение работы ЭВМ.

Есть еще мнения, вводящие в полное заблуждение, например, В.В. Крылов считает, что *в понятие нарушение работы ЭВМ следует включать любую нестандартную (нештатную) ситуацию с ЭВМ или ее устройствами, находящуюся в причинной связи с неправомерными действиями и повлекшую уничтожение, блокирование, модификацию или копирование информации*[35]. С технической точки зрения, очень расплывчато понятие *нестандартная (нештатная) ситуация*, ввиду того, что многое программное и аппаратное обеспечение не отличается исключительной надежностью и в течение дня могут давать несколько сбоев в работе, для служб технической поддержки такая ситуация является как раз стандартной или скорее *штатной*. Но более запутанной выглядит причинная связь, где неправомерные действия (не совсем ясно – какие?), являются причиной появления нестандартной ситуации, а она в свою очередь причиной последствия в виде, например, копирования информации. Хотя такая цепочка в реальной жизни действительно возможна и, с технической точки зрения, описывается как «взлом» компьютерной системы и копирование информации (в виде самостоятельного действия), но это лишь частный случай нарушения работы ЭВМ. Гораздо чаще происходит нарушение работы ЭВМ без каких-либо последствий для компьютерной информации, но

эти случаи, получается, Крылов предлагает не вносить в рамки статьи 272 УК РФ. Что по нашему мнению нельзя признать правильным потому, что «нарушение работы» являясь следствием как неправомерного доступа, так и самостоятельных действий, будет нарушать общественные отношения по законному использованию охраняемой законом компьютерной информации, даже если ничего с информацией не произошло. В связи с чем, считаем вполне оправданным шаг законодателя, поставившего нарушение работы ЭВМ (системы, сети) в один ряд с уничтожением, блокированием, модификацией или копированием информации.

Представляется, что в формулировании данного понятия ближе всего подошли С. Кочои и Д. Савельев, которые считают, что ***нарушение работы ЭВМ, системы ЭВМ или их сети** выражается в нефункционировании или неправильной работе технических устройств, являющихся частями ЭВМ (ее системы или сети), а также программ для ЭВМ, обеспечивающих и необходимых для использования охраняемой компьютерной информации*[\[36\]](#).

[\[1\]](#) Уголовное право России. Особенная часть./ Под ред. **В.Н. Кудрявцева, А.В. Наумова**. С.350.

[\[2\]](#) Уголовное право. Особенная часть// Отв. ред.: **И.Я. Козаченко, З.А. Незнамова, Г.П. Новоселов**. С.556.

[\[3\]](#) См.: [Уголовное дело №444800](#)

[\[4\]](#) **Панфилова Е.И., Попов А.Н.** Указ. соч. С. 28.

[\[5\]](#) **Андреев б.В., Пак П.Н., Хорст В.П.** Указ. соч. С. 38.

[\[6\]](#) **В. Наумов** Отечественное законодательство в борьбе с компьютерными преступлениями // <http://www.hackzone.ru/articles/a5.html>

[\[7\]](#) См.: [Уголовное дело № 9010076](#)

[\[8\]](#) Обвинительное заключение по уголовному делу № 9010076 // http://kurgan.unets.ru/~procur/my_page.htm

[\[9\]](#) **Андреев б.В., Пак П.Н., Хорст В.П.** Указ. соч. С. 38.

[\[10\]](#) *Научно-практический комментарий к Уголовному кодексу Российской Федерации в двух томах. Том второй.* – Н.Новгород: Изд. НОМОС, 1996. С. 235.

[\[11\]](#) *Комментарий к Уголовному кодексу РФ.*/ Отв. ред. **А.В. Наумов**. С. 664.

[\[12\]](#) *Комментарий к Уголовному кодексу Российской Федерации*/ Под ред. **Ю. И. Скуратова и В. М. Лебедева**. С. 699.

[\[13\]](#) Уголовный кодекс Российской Федерации. Постатейный комментарий. – М.: ЗЕРЦАЛО, ТЕИС, 1997. С 583

[\[14\]](#) **Крылов В.В.** Указ. соч. С. 47.

[\[15\]](#) *Комментарий к Уголовному кодексу Российской Федерации*/ Под ред. **Ю. И. Скуратова и В. М. Лебедева**. С. 700.

[\[16\]](#) **Крылов В.В** Указ. соч. С. 49.

[\[17\]](#) *Научно-практический комментарий к Уголовному кодексу Российской Федерации в*

двух томах. Том второй. С. 235.

[18] *Комментарий к Уголовному кодексу РФ*/ Отв. ред. А.В. Наумов С. 664.

[19] *Научно-практический комментарий к Уголовному кодексу Российской Федерации в двух томах. Том второй.* С. 235.

[20] *Комментарий к Уголовному кодексу Российской Федерации* / Под ред. **Ю. И. Скуратова и В. М. Лебедева.** С. 700

[21] *Комментарий к Уголовному кодексу РФ.*/ Отв. ред. А.В. Наумов. С. 664.

[22] **Крылов В.В.** Указ. соч. С. 50.

[23] **А. Сухарев** *Компьютерные преступления* // Домашний компьютер №7-8. 1999. С. 32.

[24] **Панфилова Е.И., Попов А.Н.** Указ. соч. С. 28.

[25] См. УК РФ.

[26] *Комментарий к Уголовному кодексу Российской Федерации*/ Под ред. **Ю. И. Скуратова и В. М. Лебедева.** С. 700-701.

[27] **Крылов В.В.** Указ. соч. С. 51.

[28] *Комментарий к Уголовному кодексу РФ.*/ Отв. ред. **А.В. Наумов.** С. 664.

[29] *Комментарий к Уголовному кодексу Российской Федерации*/ Под ред. **Ю. И. Скуратова и В. М. Лебедева.** С. 700.

[30] *Научно-практический комментарий к Уголовному кодексу Российской Федерации в двух томах. Том второй.* С. 236.

[31] **Крылов В.В.** Указ. соч. С. 51.

[32] *Комментарий к Уголовному кодексу РФ.*/ Отв. ред. **А.В. Наумов.** С. 664.

[33] *Комментарий к Уголовному кодексу Российской Федерации*/ Под ред. **Ю. И. Скуратова и В. М. Лебедева.** С. 701.

[34] *Уголовное право. Особенная часть*//Отв. ред.: **И.Я. Козаченко, З.А. Незнамова, Г.П. Новоселов.** С.558.

[35] **Крылов В.В.** Указ. соч. С. 51.

[36] **Кочои С., Савельев Д.** *Ответственность за неправомерный доступ к компьютерной информации* // Российская юстиция. 1999. № 1

§ 5. Субъективная сторона

Субъективную сторону юристы-теоретики характеризуют различно. Например, С.В. Бородин занимает крайнюю позицию и считает, что данное преступление может быть совершено только с **прямым умыслом**[1]. Этому же мнению придерживается Т.И. Ваулина, но только в отношении первого действия, поясняя, что о прямом умысле свидетельствует использование законодателем термина «неправомерный», однако, к факту наступления последствий умысел может быть как прямым, так и косвенным[2]. Близкого мнения придерживается многие юристы[3]. Но есть те, кто считает, что в отношении последствий вина может проявляться в форме неосторожности[4].

Существует и более широкое мнение, например Панфилова и Попов считают, что

преступление может быть совершено как умышленно, так и по неосторожности. Данный вывод вытекает из смысла ч. 2 ст. 24 УК РФ, поскольку в ст. 272 УК РФ специально не оговорено, что данное преступление может быть совершено только по неосторожности[\[5\]](#). Однако, именно в ч. 2 ст. 24 УК РФ сказано: *деяние, совершенное по неосторожности, признается преступлением в том случае, когда это специально предусмотрено соответствующей статьей*, но в диспозиции ст. 272 нигде нет упоминания о неосторожной вине. Следовательно, признать такую точку зрения правильной нельзя.

Итак, следует признать, что неправомерный доступ к компьютерной информации — **умышленное деяние**, поскольку в диспозиции ст. 272 УК не указано о неосторожности. Человек, пытающийся получить доступ к информации, должен сознавать, что свободный доступ к информации ограничен, он не имеет прав на доступ к этой информации. Об умысле будут свидетельствовать меры защиты информации от доступа посторонних (коды, пароли и т.п.), которые приходится преодолеть, чтобы получить доступ к информации, вывод на экран дисплея компьютера предупреждающих сообщений, устные уведомления о запрете доступа к информации и т.д. Также **умыслом** должны охватываться действия второго плана. Относительно последствий, как от самого неправомерного доступа, так и от действий второго плана, вина может быть как в форме умысла, так и в форме неосторожности.

Мотивы и цели преступления значения для квалификации по ст. 272 не имеют, но могут быть учтены при назначении наказания.

§ 6. Субъект

Субъектом преступления может быть любое вменяемое физическое лицо, достигшее 16-летнего возраста, которое совершило неправомерный доступ к охраняемой законом компьютерной информации, вызвавший указанные в законе последствия.

В ч. 2 ст. 272 УК РФ предусмотрена ответственность за то же деяние, но совершенное группой лиц по предварительному сговору, организованной группой, лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Понятие группы лиц по предварительному сговору и организованной группы дается в ст. 35 УК РФ.

Субъекты группового преступления должны выполнять полностью или частично действия, предусмотренные в диспозиции закона, т.е. обеспечивать неправомерный доступ к информации или модифицировать, уничтожать, блокировать, копировать ее. Для примера, группового преступления, можно рассмотреть ранее приведенное **уголовное дело № 9010076** [\[6\]](#) где:

Мальцев, в декабре 1998 г. вступил в преступный сговор с программистом Нефедовым для незаконного получения и использования логинов и паролей для доступа в Интернет. Мальцев через сеть Интернет, в период времени с декабря 1998 г. по июнь 1999 г. получил доступ к другим ЭВМ. Заведомо зная, что пароли к сети Интернет хранятся в файлах «rwl», Мальцев выбрал программу «PWLHACK». С помощью этой программы Мальцев совместно с Нефедовым осуществляли неправомерный доступ к охраняемой законом компьютерной информации ИКЦ «Экспресс».

В данном примере, группа лиц, в составе двух человек, по предварительному сговору, получив доступ к ЭВМ через Интернет, совместно и полностью выполнили объективную сторону неправомерного доступа к охраняемой законом компьютерной информации.

Для вменения квалифицирующего признака «совершения преступления организованной группой» необходимо установить наличие главаря (организатора, руководителя), согласованное распределение ролей при совершении преступления, внутригрупповую дисциплину, предварительное планирование преступлений (как правило), ярко выраженную направленность на занятие преступной деятельностью, устойчивость группы, связанную с длительностью ее существования, прочность связей между ее членами, наличие постоянных членов (костяка группы), совершение преступлений одним составом или с незначительными изменениями в нем. Рассмотрим пример из судебной практики:

Уголовное дело № 9983239 возбуждено 12 марта 1999 года в Управлении РОПД при ГУВД Ростовской области по ст. 272 ч.2 УК РФ. Из обвинительного заключения установлено: гр-н Шевченко, в городе Таганроге, в 1998 году, для получения и выгодного использования в коммерческой деятельности своих предприятий сведений об имуществе и дебиторских задолженностях (активах) ООО «Имикс», которые являются коммерческой тайной, создал организованную преступную группу с распределением ролей в составе подчиненных ему по роду деятельности директора ООО «Торговый Дом «ВИТ»» гр-на Безруких и референта ООО «Торговый Дом «ТАИ»» гр-на Рогова с целью незаконного получения информации, составляющей коммерческую тайну ООО «Имикс».

Являясь организатором преступной группы, с вышеуказанной целью, согласно распределению ролей, он поручил исполнителям Безруких и Рогову получить компьютер (электронно-вычислительную машину, персональную ЭВМ), принадлежащий ООО «Имикс», в базе данных которого находились сведения конфиденциального характера, который судебный пристав-исполнитель Смолин, ненадлежаще исполняя свои обязанности, передала им на хранение в не упакованном и не опечатанном виде, согласно Акту изъятия имущества от 22 октября 1998 года. Безруких и Рогов получив в служебном помещении ООО «Имикс» данную персональную ЭВМ, перевезли её в помещение ООО «Торговый Дом «ВИТ»».

Шевченко, как организатор преступной группы, поручил 22 Октября 1998 года исполнителю Безруких, произвести работы по приведению данной ЭВМ в работоспособное состояние. Безруких, используя возможность доступа к персональной ЭВМ ООО «Имикс», возникшей в результате исполнения обязанностей Хранителя в рамках Исполнительного производства, нарушая законодательство об исполнительном производстве, не принимая мер, обеспечивающих сохранение свойств, признаков и стоимости компьютера (персональной ЭВМ), принадлежащего ООО «Имикс», выполнил поручение организатора преступной группы Шевченко, при этом, в результате преступного легкомыслия гр-на Безруких, произошёл выход из строя программного обеспечения, что повлекло устойчивое создание помех для функционирования данной ЭВМ в соответствии с назначением.

Шевченко, как организатор преступной группы, поручил 22 Октября 1998 года исполнителю Рогову, произвести работы по исследованию информации в персональной ЭВМ, принадлежащей ООО «Имикс». Рогов, в период с 22 Октября 1998 года по 22 Февраля 1999 года, по согласованию с членом преступной группы Безруких, используя возможность доступа к персональной ЭВМ ООО «Имикс», маскируя свои действия исполнением работ по трудовому договору от 22 Октября 1998 года, не имея права на доступ к охраняемой

Федеральным Законом «Об информации, информатизации и защите информации» информации и информационным ресурсам ООО «Имикс», неоднократно производил доступ к компьютерной информации, содержащейся в персональной ЭВМ, при этом производил копирование этой информации на бумажные носители и гибкие диски.

Собранные незаконным путем сведения, в том числе и составляющие коммерческую тайну ООО «Имикс», накапливались организатором преступной группы Шевченко и использовались им для решения в свою пользу гражданско-правовых споров с ООО «Имикс».

Органом предварительного следствия действия Шевченко, Безруких и Рогова квалифицированы по ст. 272 ч.2 УК РФ [\[7\]](#).

О действительном наличии в данном случае организованной группы может решить только суд, рассмотрев все материалы дела. Но если выводы следователя считать верными, то мы действительно имеем случай организованной группы, созданной для совершения незаконного получения и использования сведений, составляющих коммерческую тайну (ч. 1 и 2 ст. 183 УК РФ) путем неправомерного доступа к охраняемой законом компьютерной информации (ч. 2 ст. 272 УК РФ) – то есть созданная для совершения одного или нескольких хорошо спланированных преступлений. Организованность и устойчивость группы выразилась в четких подготовительных действиях, распределении ролей и устойчивости состава до первого преступления и в достижении последующих целей. Остается непонятным, почему органом предварительного следствия данные действия Шевченко, Безруких и Рогова дополнительно не квалифицированы по ч.2 ст. 183 УК РФ, хотя явность выполненного состава очевидна.

Использование служебного положения означает, что лицо получает доступ к компьютерной информации, незаконно пользуясь права, предоставленные ему исключительно в силу выполняемой им служебной деятельности. Ярким примером использования служебного положения является рассмотренное ранее **уголовное дело № 010317**[\[8\]](#), где **Ченцов** – являясь главным специалистом по осуществлению сбыта и маркетинга, не имея права пользования компьютером и доступа в компьютерную базу головного предприятия, но используя **служебное положение** занял временно свободное рабочее место и осуществил неправомерный доступ к сети ЭВМ. Однако, в следующем примере, следователь ошибочно трактует должность Полетаева и использование служебного компьютера для неправомерного доступа, как преступления с использованием своего служебного положения. Как мы рассматривали ранее, в **уголовном деле №444800**[\[9\]](#), Полетаев, работая в должности инженера-программиста на Шадринском телефонном заводе, используя служебный компьютер через сеть Интернет зашел на жесткий диск компьютера РУФПС и просмотрев его содержимое скопировал из каталога C:\WINDOWS два файла: – user.dat и имя.pwl на компьютер, принадлежащий конструкторскому бюро Шадринского телефонного завода. Таким образом, *как считает следователь*, совершил неправомерный доступ к компьютерной информации - с использованием своего служебного положения. Но законодатель не имел в виду использование служебного положения для доступа к средству совершения преступления, служебное положение должно облегчать преступнику доступ именно к охраняемой законом компьютерной информации. В приведенном же случае, должностное положение Полетаева не облегчало ему осуществление неправомерного доступа. С таким же успехом он мог бы произвести его и с домашнего компьютера.

Повышенную уголовную ответственность за неправомерный доступ к компьютерной

информации несет также лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети. Необходимо различать лицо, имеющее доступ к ЭВМ (системе, сети ЭВМ), и лицо, имеющее право доступа к компьютерной информации. Необязательно лицо, имеющее доступ к ЭВМ, имеет право на доступ к компьютерной информации, находящейся в ЭВМ. Доступ к ЭВМ, системе ЭВМ или их сети, как правило, имеет лицо в силу выполняемой им работы, связанной с эксплуатацией или обслуживанием ЭВМ, системы ЭВМ или сети ЭВМ. Для данного случая, характерно уголовное дело № 9983239[10] приведенное в качестве примера организованной группы, где Рогов, используя возможность доступа к персональной ЭВМ ООО «Имикс», возникшую в результате исполнения обязанностей хранителя в рамках исполнительного производства, неоднократно производил неправомерный доступ к охраняемой законом компьютерной информации.

Есть и обратный пример уголовного дела, приведенного в начале данного параграфа, где *Федоров, используя компьютер, без ведома и разрешения владельца, вышел в глобальную сеть Интернет и произвел несанкционированную модификацию программы публичного поискового сервера НовГУ. Данное деяние квалифицировано как неправомерный доступ, совершенное лицом, имеющим доступ к ЭВМ, системе ЭВМ и их сети.* Здесь следователь **ошибочно** считает, что лицо, имеющее доступ к ЭВМ, подключенному к сети Интернет имеет доступ к сети ЭВМ, где хранится охраняемая законом компьютерная информация. Сеть Интернет, хоть и является сетью ЭВМ в техническом смысле, между тем, имеет черту, выводящую ее за рамки обыкновенной сети ЭВМ, - это глобальность, т.е. распространение во всем мире. Хотя юридически у данной сети нет определения и нет единого понимания, все же не стоит ее сравнивать с сетью или системой ЭВМ. Представляется правильным, на данном этапе, воспринимать Интернет, как единое *информационное пространство*, не имеющее ни собственника, ни владельца, ни государственную принадлежность.

[1] *Комментарий к Уголовному кодексу РФ.*/ Отв. ред. **А.В. Наумов.** С. 665.

[2] *Уголовное право. Особенная часть*/ Отв. ред.: **И.Я. Козаченко, З.А. Незнамова, Г.П. Новоселов.** С. 558.

[3] **Гульбин Ю.** *Преступления в сфере компьютерной информации* // Российская юстиция. 1997. № 10

[4] **Андреев б.В., Пак П.Н., Хорст В.П.** Указ. соч. С. 37.

[5] **Панфилова Е.И., Попов А.Н.** Указ. соч. С. 28.

[6] См.: [Уголовное дело № 9010076](#)

[7] Обвинительное заключение по уголовному делу № 9983239// http://kurgan.unets.ru/~procur/my_page.htm

[8] См.: [уголовное дело № 010317](#)

[9] См.: [уголовном деле №444800](#)

[10] См.: [уголовное дело № 9983239](#)

Заключение

С повышением роли информации во всех сферах человеческой деятельности повышается роль и значение компьютерной информации как одной из популярных форм создания, использования, передачи информации. А с повышением роли компьютерной информации требуется повышать уровень ее защиты с помощью технических, организационных и особенно правовых мер.

С 1992 года законодатель начал вводить правовое регулирование в сфере использования компьютерной информации, но как показали исследования данной работы, не всегда последовательное. В частности, несоответствие терминологии различных законов, например, несоответствие сути термина «информация» употребленного в Законе об информации и Уголовном законе. Отсутствие, законодательного закрепления некоторых терминов употребляемых в Уголовном законе, например, «ЭВМ», «система ЭВМ», «сеть ЭВМ», «копирование информации» и других. Непоследовательность обнаруживается и в самом Уголовном законе, например, при нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети упоминается о последствиях в виде уничтожения, блокирования или модификации информации, но ничего не говорится о нарушении работы ЭВМ, системы ЭВМ, их сети, хотя это, как и в двух других составах предусмотренных Уголовным кодексом, может принести собственнику ущерб. Также нужно сказать о непоследовательном подходе к формированию квалифицирующего признака о неосторожном причинении тяжких последствий. Такой признак предусмотрен в двух статьях 273 и 274 УК РФ, а это нельзя признать верным, т.к. неосторожное причинение тяжких последствий в равной степени может быть следствием всех трех незаконных деяний.

Проведенные исследования подводят к выводу необходимости внесения значительного массива дополнений и изменений в действующее законодательство. Также издания новых законов вносящих правовое регулирование в информационные отношения, обусловленные распространением на территории России глобальной сети Интернет.

Также проведенные в работе исследования показали, что проработка вопросов в юридической литературе об информационных отношениях, в общем, и компьютерных преступлений в частности, находится на низком уровне. Многие суждения, как в техническом плане, так и в юридическом плане, далеки от практики. Некоторые приводимые мнения только запутывают, нежели помогают разобраться. В связи с чем, в работе приведены собственные мнения по некоторым вопросам, в частности, по формулировке понятия «ЭВМ», «системы ЭВМ», «компьютерного преступления», «неправомерного доступа» и других.

В настоящее время крайне необходимо более глубокое теоретическое осмысление нового законодательства об информационных отношениях, в частности об ЭЦП, внесённых новелл и практики применения. Необходимо поднять многие дискуссионные вопросы для обсуждения, как в рамках специализированных конференций, так и в Интернет-конференциях и Интернет-форумах.

Анализ судебной и следственной практики показал, что следователи и суды практически не имеют знаний в юридических и технических вопросах компьютерных преступлений и действуют по аналогии, что приводит к неправильной квалификации и необоснованным приговорам. Хотя при территориальных органах управления внутренних дел созданы

подразделения по борьбе с преступлениями в сфере высоких технологий, но работают там сотрудники по большей части недостаточно квалифицированные либо в технической стороне, либо в юридической стороне компьютерного преступления. В связи с чем, требуется осуществить организационные и правовые меры:

- по подбору в данные подразделения только специалистов в обеих областях, либо подготовке таких специалистов и дальнейшее постоянное и динамичное повышение их квалификации;
- закрепить, в рамках подведомственности, дела о компьютерных преступления только за этими подразделениями;
- разработать научные методики, программные средства и технические устройства для получения и закрепления доказательств совершения компьютерного преступления;
- и другие меры.

Итогом проведенных исследований в работы является разработка ключевых положений, характеризующих понятие компьютерного преступления и неправомерного доступа к компьютерной информации. Данные положения могут служить базой для дальнейших исследований или методическим материалом в правоприменительной практике.

Список использованной литературы

Нормативная база:

1. Конституция РФ. – М.: ИНФРА-М-НОРМА, 1997.
2. Уголовный кодекс Российской Федерации (с изм. и доп. на 01.10.2001).//М.: ООО «ВИТРЭМ», 2001.
3. Уголовный кодекс РФ. Особенная часть. Проект // Юридический вестник. 1994. № 22-23.
4. Уголовный кодекс РФ. Проект // Юридический вестник. 1995. № 7-8.
5. Гражданский кодекс Российской Федерации (часть первая) от 21.10.94 г. № 51-ФЗ // Российская газета. № 238-239. 08.12.94
6. Федеральный закон «Об информации, информатизации и защите информации» от 20.02.1995 г. // Собрание законодательства РФ. 1995. № 8. ст. 609.
7. Федеральный закон «Об участии в международном информационном обмене» от 05.06.96 № 85-ФЗ. // Российская газета. № 129. 11.07.96
8. Закон РФ «Об авторском праве и смежных правах» от 09.07.93 № 5351-1 // Российская газета. № 147. 3 АВГ. 1993
9. Закон РФ «О правовой охране программ для ЭВМ и баз данных» от 23.09.92 №3526-1 // Российская газета, № 230. 21.10.92.
10. Закон РФ «О правовой охране топологий интегральных микросхем» от 23.09.92 №3523-1 // Российская газета, № 229. 20.10.92.
11. Закон РФ «О государственной тайне» от 21.07.93 № 5485-1// Российская газета. № 182. 21.09.93
12. Закон РФ «Об обязательном экземпляре документов» от 23.11.94 № 77-ФЗ //

Российская газета. № N 11-12. 17.01.95

13. Закон РФ «О связи» от 21.07.93 № 5485-1// Российская газета. № 211 от 14.09.93

14. Об утверждении перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 г. № 188 // Собрание законодательства РФ. 1997. №10. ст. 1127.

Комментарии и учебники:

15. *Постатейный комментарий к части первой ГК РФ*// Гуев А.Н. – М.: Инфра*М, 2000.

16. *Комментарий к Уголовному кодексу РФ.*/ Отв. ред. А.В. Наумов. – М.: Юристъ, 1997.

17. *Комментарий к Уголовному кодексу Российской Федерации. Особенная часть* // Под ред. Ю. И. Скуратова и В. М. Лебедева. – М.: Издательская группа МНФРА М – НОРМА, 2001.

18. *Научно-практический комментарий к Уголовному кодексу Российской Федерации в двух томах. Том второй.* – Н.Новгород: Изд. НОМОС, 1996.

19. *Уголовный кодекс Российской Федерации. Постатейный комментарий.* – М.: ЗЕРЦАЛО, ТЕИС, 1997.

20. *Уголовный кодекс Российской Федерации (с постатейными комментариями).* – М.: ЗАО «Изд-во ЭКСМО-Пресс», 1998.

21. *Уголовное право России. Особенная часть.*/ Под ред. В.Н. Кудрявцева, А.В. Наумова. – М.: Юристъ, 2000.

22. *Уголовное право. Особенная часть*// Отв. ред.: И.Я. Козаченко, З.А. Незнамова, Г.П. Новоселов- М.: Изд. НОРМА-Инфра*М, 1998.

Статьи и монографии:

23. Андреев Б.В., Пак П.Н., Хорст В.П. *Расследование преступлений в сфере компьютерной информации.*// М.: ООО Изд. «Юрлитинформ», 2001.

24. Батурин Ю.М., Жодзишский А.М. *Компьютерная преступность и компьютерная безопасность.*// М.: Юрид. лит., 1991.

25. Гульбин Ю. *Преступления в сфере компьютерной информации* //Российская юстиция. 1997. № 10

26. Коржов В. *Право и Интернет: теория и практика* // [Computerworld \(Россия\), №43, 1999](http://www2.osp.ru/cw/1999/43/06.htm). Интернет версия:<http://www2.osp.ru/cw/1999/43/06.htm>

27. Кочои С., Савельев Д. *Ответственность за неправомерный доступ к компьютерной информации* // Российская юстиция. 1999. № 1.

28. Крылов В.В. *Информация как элемент криминальной деятельности* // Вестник Московского университета, Серия 11, Право – 1998. № 4.

29. Крылов В.В. *Информационные преступления - новый криминалистический объект* // Российская юстиция. 1997. № 4

30. Крылов В.В. *Информационные компьютерные преступления*// М.: изд. Инфра-М-Норма, 1997.

31. LENTA.RU *В суд за ссылку: новгородская версия* // Материалы Интернет-страницы: http://lenta.ru/internet/2000/02/03/porno/_Printed.htm

32. Максимов В.Ю. *Компьютерные преступления(вирусный аспект)*// Ставрополь: Кн. Изво, 1999.
33. Материалы «Большой Энциклопедии Кирилла и Мефодия 2001» // 2CD «Кирилл и Мефодий». 2001 г.
34. Наумов В. *Отечественное законодательство в борьбе с компьютерными преступлениями* // <http://www.hackzone.ru/articles/a5.html>
35. Панфилова Е.И., Попов А.Н. *Компьютерные преступления: Серия «Современные стандарты в уголовном праве и уголовном процессе»* // Науч. редактор проф. Б.В. Волженкин. СПб., 1998.
36. Сальников В.П., Ростов К.Т., Морозова Л.А., Бондуrowsкий В.В. *Компьютерная преступность: уголовно-правовые и криминологические проблемы (международная научно-практическая конференция)*//Государство и право. 2000. № 9.
37. Симкин Л. *Как остановить компьютерное пиратство?* // Российская юстиция. 1996. № 10
38. Сорокин А.В. *Компьютерные преступления: уголовно - правовая характеристика, методика и практика раскрытия и расследования*// http://kurgan.unets.ru/~procur/my_page.htm,1999.
39. Сухарев А. *Компьютерные преступления* // Домашний компьютер, №7-8, 1999.
40. Ушаков С.И. *Преступления в сфере обращения компьютерной информации(теория, законодательство, практика)*// Автореферат кандидатской диссертации. – Рост. –н-Д.: Рост. юр. инст. МВД РФ, 2000.
41. Яблоков Н.П. *Криминалистическая характеристика финансовых преступлений* // "Вестник Московского университета", Серия 11, Право - 1999. № 1.

Практика:

42. Обвинительное заключение по уголовному делу № 73129// http://kurgan.unets.ru/~procur/my_page.htm
43. Обвинительное заключение по уголовному делу № 77772// http://kurgan.unets.ru/~procur/my_page.htm
44. Обвинительное заключение по уголовному делу № 011678 // http://kurgan.unets.ru/~procur/my_page.htm
45. Обвинительное заключение по уголовному делу № 010317 // http://kurgan.unets.ru/~procur/my_page.htm
46. Обвинительное заключение по уголовному делу № 444800 // http://kurgan.unets.ru/~procur/my_page.htm
47. Обвинительное заключение по уголовному делу № 30 // http://kurgan.unets.ru/~procur/my_page.htm
48. Обвинительное заключение по уголовному делу № 9010076 // http://kurgan.unets.ru/~procur/my_page.htm
49. Обвинительное заключение по уголовному делу № 9983239// http://kurgan.unets.ru/~procur/my_page.htm

