Содержание

Введение

Данная работа посвящена правовым проблемам борьбы мошенничества с использованием всемирной компьютерной сети Интернет.

Актуальность темы требует подробного комментария.

Технический прогресс, как известно, имеет много положительных сторон, однако на этом пути человечество подстерегают и серьезные опасности. Данное утверждение справедливо, в частности, по отношению к развитию компьютерной техники. Конечно, рано или поздно практически все нежелательные последствия выявляются, после чего предпринимаются меры для их нейтрализации, но гораздо разумнее просчитать ситуацию заранее и постараться предотвратить все негативное. Важность и целесообразность прогнозирования различных вариантов развития событий пропорциональна их значимости.

Сказанное прежде всего относится к такому явлению, как преступность. Надо отдать должное нашим соотечественникам, которые давно обратили внимание на криминальные явления, сопровождающие процесс компьютеризации, который давно начался за рубежом. Когда большинство наших соотечественников имело очень смутное представление о вычислительной технике, в юридической и другой специальной литературе уже появились статьи сначала информационного, а затем и предостерегающего характера. Заслуга авторов подобных материалов заключается в том, что они своевременно предупредили о грозящей опасности. В частности, заинтересованные лица были осведомлены о большой вероятности распространения у нас хищений денежных средств с использованием возможностей электронно-вычислительной техники.

В этом состоит единственная положительная сторона российского отставания в области распространения средств электронно-вычислительной техники. На основе чужого опыта мы имеем возможность определять вероятное ближайшее, а также более отдаленное во времени состояние

нового вида преступности, тенденции и динамику его развития, изменения качественных характеристик.

Прогнозы, касающиеся компьютерной преступности, к сожалению, сбылись, и сегодня мы уже без прежнего удивления узнаем из сообщений криминальной хроники о хищениях или попытках хищений с использованием электронных средств доступа. Как зарубежный, так и отечественный опыт свидетельствуют о значительной опасности нового вида преступности. Так, по данным американского ФБР, усредненные показатели убытков от каждого такого преступления превышают 600 тыс. долларов США, что, по меньшей мере, в шесть-семь раз больше среднестатистического ущерба от вооруженного ограбления банка.

Заинтересованные лица в России, своевременно предупрежденные о существующей опасности, имели возможность подготовиться, чтобы в нужный момент быть во всеоружии. Это позволило не допустить обвального роста хищений, совершаемых посредством электронных средств доступа. Большинство банков и других учреждений, использующих в работе электронно-вычислительную технику, всеми возможными способами обезопасили себя, применив многоуровневые системы охраны компьютерной информации от несанкционированного доступа, а также иные средства защиты. Предвидение возможных рисков позволило избежать материального ущерба и других нежелательных последствий.

Целью данной работы является характеристика проблем квалификации мошенничества с использованием сети Интернет. Задачи работы могут быть сформулированы в следующем виде:

1. Дать характеристику сети Интернет как объекта правового регулирования и оценить её «криминальный» потенциал, т.е. возможность совершения тех или иных преступлений с её использованием.
2. Оценить возможности и квалифицировать виды мошенничества с использованием сети Интернет. Наиболее распространённые способы –

размещение ложной информации с целью обмана, операции с безналичными переводами и с ценными бумагами.

3. Определить возможности борьбы с мошенничеством в Интернете.

Работа состоит из трёх глав. В первой главе даётся характеристика Интернета с правовой точки зрения. Во второй главе производится квалификация мошенничества как обманного хищения (устанавливаются общие признаки хищения, обман как обязательный признак мошенничества – в работе используется даже устоявшийся термин «обманные хищения»), затем даётся классификация мошенничеств в случае использования Интернета, при этом особое внимание уделяется денежным переводам и мошенничеству на рынке ценных бумаг. Третья глава посвящена проблемам борьбы с мошенничеством в Интернете.

Нормативно-правовые акты, использованные в качестве источников для написания работы, - это, естественно, Уголовный кодекс РФ (в том числе его специальное издание с постатейными комментариями Ю.И. Скуратова и В.М. Лебедева), а также ряд Постановлений Пленумов Верховного Суда СССР и Российской Федерации. Теоретические вопросы уголовного права даются по двухтомнику Б.В.Здравомыслова «Уголовное право Российской Федерации».

Однако главные источники для написания работы-публикации: «Расследование хищений, совершаемых в кредитно-финансовой сфере» (авторы - В.Г. Баяхчев и В.В. Улейчик); «Преступное посягательство на имущество» (автор - П.С. Яни); «Собственность и имущественные отношения в уголовном праве» (автор - А.П. Безверхое); «Имущественные преступления: сравнительно-правовой аспект» (автор - И.А. Клепицкий). Так как все эти публикации взяты из журналов «Законодательство. Право для бизнеса», подавляющее большинство практических примеров в работе относятся к сфере бизнеса (по «обманным» хищениям - почти все примеры).

Примеры взяты частично из публикации П.С. Яни, частично из публикации А.Г. Безверхова. Следует обратить внимание и на построение

работы (в ней нет «теоретических» и «практических» частей, а вместо этого примеры с комментариями приводятся по всей работе, т.е. теория чередуется с практикой), и на подбор примеров (в большинстве из них как раз говорится о ситуациях, когда нет хищения, т.е. понятие и признаки хищения выводятся «доказательством от противного» - методом исключения того, что хищением не является).

В связи с наличием примеров из бизнеса «справочным» источником для работы выступает «Гражданское право» (под редакцией А.П. Сергеева и Ю.К. Толстого), а один раз - и «Информационное право» (автор -В.А. Копылов). В работе затрагиваются и некоторые дискуссионные вопросы (например, о корыстном мотиве).

Заключение к работе содержит краткие выводы и одновременно является авторефератом работы.

Отметим, что Постановления Пленума Верховного Суда СССР, упоминаемые в данной работе, являются действующими в той части, в какой они не противоречат уголовному законодательству РФ (известны и более ранние действующие постановления; например, в отношении определений длящихся и продолжающихся преступлений продолжает применяться Постановление Верховного Суда СССР, датированное 1929 годом).

Глава I. Всемирная сеть Интернет как объект правового регулирования

1.1."Интернет" в современном мире.

О глобальной компьютерной сети (ее другая обобщающая характеристика - всемирная информационная служба), известной под английским названием INTERNET, часто говорят, что ее возникновение и непредсказуемо бурное развитие может стать крупнейшим событием в истории мировой цивилизации конца XX в. Не будем спорить, насколько соответствует такая оценка действительному положению вещей, но вряд ли еще к какому-либо аспекту развития компьютерных технологий было привлечено столь пристальное внимание не только узких специалистов, но и все возрастающего числа людей самых разных профессий.

Самое простое определение "Интернета" - объединение компьютерных сетей. А их существует множество - от локальных (например, объединяющих несколько компьютеров на одном предприятии) до региональных и общенациональных коммерческих сетей (например, "Америка он-лайн" (АОЛ) или "Компьюсерв" в США). Интернет имеет много общего с обычными сетями типа АОЛ. Клиенты ("пользователи" или "подписчики") "Интернета" так же могут подключаться к другим компьютерам, обмениваться сообщениями по электронной почте, получать разнообразную информацию с многочисленных баз данных. Но интернет имеет и существенные отличия от исторически предшествовавших ему коммерческих сетей, что и обеспечило ему столь стремительное развитие в последние годы.

Во-первых, "Интернет" организационно не является чем-то единым целым. У него нет владельца или владельцев, продающих содержащуюся в нем информацию. Этим занимаются особые организации - производители информации, имеющие возможность доступа к "Интернету" на практически тех же условиях, что и потребители информации.

Во-вторых, "Интернету" присущи подлинно глобальные масштабы - он объединяет компьютерные сети абсолютного большинства стран мира. Любой желающий подключиться к "Интернету" может стать его подписчиком, если у него имеются компьютер, модем, телефонная линия и сравнительно небольшая сумма денег. К концу 1996 г. число пользователей "Интернета" во всем мире уже исчислялось десятками миллионов, и ежедневно подключаются десятки тысяч новых клиентов.

В-третьих, сложилось так, что среди всех компьютерных сетей именно "Интернет" постоянно и успешно прогрессирует в своем развитии не только "вширь" (за счет постоянно растущего числа пользователей), но и "вглубь" (путем увеличения количества оказываемых услуг и объемов циркулирующей по сети информации).[1]

Непосредственным предшественником "Интернета" была компьютерная сеть APRANET Министерства обороны США, объединившая в 1969 г. несколько американских университетов и компаний, выполнявших военные заказы. Она создавалась для использования, например, в случае военных конфликтов. Сеть оказалась вполне надежной и удобной, особенно для оперативного обмена результатами научных исследований, и к ней стали подключаться другие компьютеры, в первую очередь различных университетов США. Объем чисто гражданских вопросов, решавшихся через эту сеть, постоянно рос, и Министерство обороны США разделило сеть на две части: одну для военных целей, другую - для гражданских. Они были связаны набором технических и программных средств, составивших так называемый Internet Protocol (межсетевой протокол). Так появилось само название "интернет".

Постепенно к сети стали подключаться частные компании, некоторые из них продавали возможность входа в сеть всем желающим. "Интернет" был приватизирован. Правительство США перестало его субсидировать и

[1] Калятин В.О Проблемы установления юрисдикции в Интернете //Законодательство, N 5, май 2001 г. С. 32

контролировать. С начала 90-х гг. он стал лавинообразно распространяться по странам и континентам, включая в себя все новые локальные сети и базы данных. Такие сети подключаются к более крупным сетям, которые для соединения друг с другом имеют так называемые точки встречи (meeting point).

Если какое-либо предприятие или частное лицо желает стать клиентом Интернета, ему необходимо обратиться с просьбой о подключении к специальным поставщикам (provider) сети - организациям, имеющим прямые входы в сеть (как правило, через телефонные или оптоволоконные кабели). Ими могут быть университеты, специализированные фирмы, телефонные компании и др. На территории стран СНГ обычно это фирмы, имеющие возможность подключения к АТС или ведомственным каналам связи, обеспечивающим скоростную передачу данных. Именно поставщик - то лицо, с которым пользователь "Интернета" непосредственно вступает в отношения по поводу применения сети. Получая возможность подключения к компьютеру поставщика, пользователь тем самым включает собственный компьютер в своего рода локальную сеть (сеть поставщика), которая соединена с другими сетями, образующими интернет.

Для подключения к "Интернету" новый клиент должен зарегистрировать свое имя (можно выбрать его произвольно, однако оно не должно совпадать с уже имеющимися), приобрести необходимое программное обеспечение и арендовать линию связи. Эти и другие услуги поставщиков платные, но они имеют постоянную тенденцию к удешевлению. Сейчас аренда одного часа работы телефонного канала стоит примерно 1 доллар США. Впрочем, в некоторых странах поставщики-монополисты могут предлагать свой "товар" существенно дороже.

Оплата услуг производится подобно оплате за междугородные телефонные разговоры, как правило, раз в месяц. Подсчет времени, затраченного клиентом на работу в "Интернете", осуществляет поставщик.

Если пользователь обращается лишь к бесплатным ус лугам сети, то его затраты ограничиваются оплатой счетов поставщика.

В настоящее время большое количество услуг клиенты получают бесплатно. Например, при обмене данными между сетями оплачивается лишь использование каналов передачи информации, но не сама информация. Конечно, со временем могут произойти изменения.

Необходимо помнить, что сама сеть никаких услуг, помимо подключения друг к другу компьютеров, оказывать не может. Все услуги в "Интернете" предоставляются различными организациями. Некоторые из них вообще не имеют отношения к компьютерным технологиям, другие специализируются на сетевых услугах, например, создавая и размещая в "Интернете" рекламу других фирм или публикуя сетевые версии газет и журналов. Многие организации и частные лица оказывают услуги в рекламных целях. Ряд фирм, ведущих активную коммерческую работу в интернете, хорошо известен и в "некомпьютерном" мире. Так, крупные авиакомпании не только предлагают потенциальным пассажирам в течение сеанса разработать маршрут авиапутешествия, но и сразу же купить билет.[2]

В целом можно сказать, что в "Интернете" уже доступна, или в скором времени будет доступна, практически любая услуга, которую можно получить без непосредственного контакта с производителем (например, по телефону): справочная информация, прогноз погоды, консультация юриста, заказ и покупка мебели по каталогу, просмотр видеофильмов и т. д. При этом все соединения между компьютерами происходят практически мгновенно, и только плохое качество каналов связи или недостаточная мощность компьютера могут задержать прохождение ответа до нескольких секунд.

И, конечно, главное предназначение "Интернета" - осуществлять связь между людьми, а не между их компьютерами. Пользователи сети могут обмениваться письменными сообщениями, компьютерными программами,

[2] Якушев М. А. Интернет и право //Законодательство, 1997, N 1 С. 25

рисунками, фотографиями. Появилась даже возможность двустороннего аудиоконтакта: специальная программа позволяет преобразовывать звуковые сигналы для их передачи и последующего обратного преобразования в звук на компьютере собеседника. Если субъекты находятся в разных городах или странах, то оплачивается не междугородный или международный телефонный разговор, а только аренда канала связи у местных поставщиков (то есть вместо нескольких долларов США в минуту всего около 1 доллара в час.)

Программные средства для "Интернета" развиваются и устаревают настолько быстро, что трудно даже представить, какие возможности появятся у его пользователей всего через несколько лет. Но можно уверенно предсказать, что "Интернет" не только станет мощным фактором, стимулирующим индустрию связанных с ним услуг, но и войдет в повседневную практику любой организации и в жизнь семьи. Причем это наверняка произойдет и в тех странах, где современный уровень развития средств связи недостаточен для устойчивой работы компьютерных сетей, а уровень доходов средней семьи пока не позволяет ей планировать покупку персонального компьютера[3].

1.2. "Интернет" с правовой точки зрения

"Интернет" пока еще мало исследован с точки зрения юридической специфики отношений, возникающих в связи с его существованием и практическим применением. И прежде всего предстоит решить два вопроса принципиального характера.

Первый - о юридической природе самого "Интернета". Что это - субъект права, вступающий в различные отношения со своими клиентами,

[3] Копылов В.А. Информационное право. М.: Юристь, 2002- С. 112

или объект правоотношений, природу которых еще только предстоит уточнить?

Второй вопрос - о праве, применимом к этим правоотношениям. Если оно существует, то какая нормативная база его составляет, к какой системе и отрасли эти правовые нормы можно отнести? Если его до сих пор нет, то на чем же основывалось развитие "Интернета" до настоящего времени и что стоило бы предпринять в этом отношении в будущем?

Кроме того, можно выделить множество частных проблем. Они либо уже возникали в процессе использования интернета, либо в ближайшее время неизбежно заявят о себе. В конечном итоге вопросы, связанные с функционированием интернета, затрагивают огромные материальные, информационные, людские ресурсы и соответствующие объемы денежных средств. Все это не может остаться без внимания публичной власти, а значит, и без принятия нормативного регулирования в этой сфере.

Уже отмечалось выше, что "Интернет" не является чем-то единым. Ни в одной стране мира не существует организационной структуры, выступающей в качестве единоличного собственника или владельца данной компьютерной сети.

Не является владельцем "Интернета" и федеральное Правительство США, практически прекратившее субсидирование даже отдельных сетей на территории государства. Не имеет уже отношения к "Интернету" и Министерство обороны США, владеющее собственной засекреченной компьютерной сетью.

Для обычного клиента представителем того, что он называет "Интернет", выступает поставщик, предоставляющий ему канал связи с соответствующим программным обеспечением. В тех случаях, когда клиент совершает возмездную сделку во время сеанса связи в "Интернете" (например, подписывается на заинтересовавший его журнал в электронной версии), он знает, что его контрагентом выступает не поставщик, а организация, предоставляющая указанную услугу (издательская фирма или

редакция), поскольку по сути такая сделка соответствует процессу обычной, "некомпьютерной" подписки на печатные издания.

Для фирмы-производителя сетевых услуг представителем "Интернета" являются специализированные компании, способные разместить предлагаемую производителем информацию на своих компьютерах (называемых серверами) и сделать ее доступной для других пользователей сети (на условиях фирмы-производителя). Такая специализированная компания (владелец сервера) часто одновременно является и поставщиком, но так бывает не всегда, и в этом случае владелец сервера входит в "Интернет" на общих основаниях.

Для поставщика представителем "Интернета" выступают более крупные сети, предоставляющие ему возможность соединения с ними. У каждой из таких сетей есть собственный владелец, но, конечно, по отдельности ни один из них все сети, объединяемые Интернетом, ни технически, ни юридически контролировать не может.

Представители наиболее крупных сетей "Интернета" объединены в несколько организаций так называемого "сообщества "Интернет". Однако эти организации не являются органами управления сетью. Они занимаются в первую очередь согласованием технических стандартов (обмена данными, соединения сетей и т.д.), а также регистрацией так называемых узловых компьютеров (соединенных между собой точками встречи) и доменных адресов или имен (идентификационных названий таких компьютеров). Само по себе это очень важно для технического функционирования сети, но недостаточно для управления организацией.

Все вышесказанное подтверждает, что у "Интернета" невозможно выделить признаки, обычно характеризующие юридическое лицо. "Интернет" не обладает организационным единством, не инкорпорирован ни в одной из стран мира и не создан как международная организация. "Интернет" не имеет собственного обособленного имущества, так как используемые в нем материальные и информационные ресурсы принадлежат

на праве собственности самым разным субъектам (каналы связи - телекоммуникационным компаниям; компьютеры, производящие подключение к сети - поставщикам; компьютеры клиентов - самим клиентам; техническое и программное обеспечение работы магистральных сетей - владельцам таких сетей; распространяемая на коммерческих условиях информация - ее производителям и прочим владельцам). Не способен "Интернет" и иметь какие-либо самостоятельные права и нести обязанности, так как за каждым возникающим при работе в Интернете правоотношением стоит конкретный правоспособный субъект. Скажем, при подключении клиента к сети его контрагентом выступает поставщик, при покупке через сеть какого-либо товара (например, информации о рынке недвижимости, либо самой недвижимости) соответствующая организация-продавец, а при производстве платежа по сделке через сеть - специализированная финансовая фирма (например, так называемый виртуальный банк)[4].

Легко заметить, что во всех возникающих правоотношениях и взаимодействующие субъекты, и характер их ответственности совершенно различны. Иначе говоря, "Интернет" однозначно не является ни зарегистрированной организацией, ни юридическим лицом вообще.

Является ли "Интернет" каким-либо субъектом права "нового типа", для которого хотя и неприменимы традиционные признаки юридического лица, (например, организационное единство), но можно сконструировать нечто, способное свидетельствовать о его "субъектности"? Подобные идеи иногда высказываются участниками дискуссий на юридические темы в самом "Интернете" (студентами факультетов права американских университетов). В частности, предложено понятие "множественности субъектного состава" интернета, позволяющее якобы наделить последний характеристикой нового субъекта права.

Мнение о "новизне" "Интернета" как субъекта права представляется безосновательными. Поскольку он не является юридическим лицом, а

[4] Демьянова К. Интернет - средство массовой информации? // Законодательство, N 9, сентябрь 2000 - С.17

организации, вступающие в вышеуказанные правоотношения, способны самостоятельно осуществлять свои права и нести обязанности, нет никакой необходимости искусственно соединять их в некий "множественный субъект". Множественность субъектов конкретного обязательства может существовать (в том числе и в интернете), но к вопросу о субъектах права это отношения не имеет.

Итак, "Интернет" не является субъектом права, т. е. участником правоотношений, но, может быть, "Интернет" - объект права, т. е. то, по поводу чего правоотношения возникают?

Попытаемся рассмотреть уже приводившиеся примеры правоотношений по поводу работы в "Интернете" с целью выявления их предметного основания. Подключение компьютера клиента к локальной сети поставщика осуществляется путем совершения нескольких юридически значимых действий, природа которых хорошо известна и не является чем-то исключительным - продажа программного (программы входа в интернет) и аппаратного обеспечения (модем); аренда канала связи (можно провести аналогию с продажей машинного времени на ЭВМ или с использованием телефонной линии при междугороднем разговоре). Иначе говоря, используются договор купли-продажи, договор аренды, а также в определенной степени нормы об охране исключительных прав на предоставленное программное обеспечение (его нельзя переустановить еще на один компьютер без регистрации нового пользователя). В случае покупки какого-либо товара через сеть опять-таки применяются достаточно теоретически проработанные понятия - договор купли-продажи, право собственности на продаваемый товар и т. д. Даже в случае не только сетевой купли-продажи, но и сетевой оплаты (например, с применением так называемых условных электронных денег) предмет и специфика расчетных отношений хорошо знакомы хотя бы специалисту в области безналичных расчетов кредитными карточками.

Другими словами, правовые отношения порождает не "Интернет" как компьютерная сеть, а сами объекты, которые тем или иным образом связаны с такой сетью. Эти объекты либо уже хорошо известны (товары, выставленные на продажу по каталогу), либо менее исследованы с точки зрения юридической науки, но не представляющие собой чего-то необычного (например, информация в том или ином виде или услуги по размещению рекламных страниц на серверах). Это легко объяснимо: "Интернет" как компьютерная сеть не создает каких-либо новых объектов и товаров, а лишь предоставляет возможности для их создания, размещения и реализации между пользователями сети.

Что же касается отношений, которые возникают в связи с функционированием "Интернета" именно как компьютерной сети (имеются в виду технические - аппаратные и программные - средства соединения компьютеров), то, во-первых, они практически не носят правового характера, а относятся к сфере технических стандартов и спецификаций. Во-вторых, в тех немногих случаях, когда то или иное правовое регулирование все же применяется, его предметом становятся опять-таки услуги, субъективные права и материальные объекты, ничем принципиально не отличающиеся от аналогичных предметов регулирования, существовавших и до появления сети "Интернет" (например, прокладка кабелей связи, выделение под них земельных участков, порядок производства соответствующих работ; право собственности владельцев отдельных сетей на подсоединяемые компьютеры; порядок использования телефонных линий, принадлежащих телекоммуникационным компаниям). Все эти вопросы либо уже детально регламентированы соответствующими (и достаточно многочисленными) правовыми актами, либо для их урегулирования в будущем достаточно применить методы, аналогичные уже существующим[5].

Мы приходим к единственно возможному выводу - сам по себе "Интернет" как компьютерная сеть не является каким-либо новым объектом

[5] Якушев М. А. Как отрегулировать Интернет? //Законодательство, N 9, сентябрь 2000 – С. 31

права, который можно было бы поставить в один ряд, например, с регулированием исключительных прав, права собственности или деликтной ответственности. Не может быть "Интернет" в строгом смысле и объектом гражданского права подобно имуществу, информации или правам на результаты интеллектуальной деятельности.

Впрочем, это не исключает возможности появления в будущем неких факторов социальной жизни, которые благодаря развитию "Интернета" потребуют специфической регламентации в рамках отдельного отраслевого (или более частного) регулирования. (Подобно тому, как сто-двести лет назад выявилась социально значимая проблема, связанная с охраной прав авторов литературных произведений, что к настоящему времени привело к созданию целого нормативного массива, относящегося к так называемым исключительным правам, "интеллектуальной собственности". К сожалению, пока еще преждевременно предполагать, что именно может потребовать столь принципиального изменения точки зрения на "Интернет" в целом как на возможный объект права.

Может быть, раз "Интернет" не является ни объектом, ни субъектом права, разговор о какой-либо юридической специфике его функционирования является вообще беспредметным?

Конечно же, это не так. Специфика отношений, связанных с работой в сети "Интернет", безусловно, имеется. Его появление и развитие вносит много принципиально нового в характер взаимоотношений между людьми и организациями, связывающимися между собой через сеть, а также влечет возникновение новых деятельных субъектов-производителей сетевых услуг. Скорее всего, юридическая особенность отношений между пользователями "Интернета" (как и отношений по поводу производимых в сети действий) заключается в специфическом способе реализации прав и обязанностей лиц - пользователей сети. Чтобы пояснить указанную мысль, для примера рассмотрим с точки зрения применяемого регулирования обычный

телефонный разговор, в общих (технических) чертах сходный с сеансом работы в Интернете.

Создает ли сам факт телефонного разговора какие-либо права и обязанности для собеседников? Разумеется, нет, поскольку не существует нормативных правил, которые бы регулировали порядок ведения телефонных разговоров. Значит, телефонный разговор объектом правового регулирования быть не может. Сделаем лишь две оговорки. Во-первых, имеется ряд правил рекомендательного характера (не занимать долго линию, не оставлять трубку неповешенной и т. д.). Но эти правила чаще всего связаны с технической проблемой загруженности линий (а вопрос о лаконичности телефонных разговоров чаще всего снимается введением повременной оплаты телефонных переговоров), и лишь в случае так называемого "телефонного хулиганства" влекут за собой применение административной и иной ответственности (которая в целом мало отличается от ответственности за хулиганские поступки "не по телефону"). Во-вторых, в ряде организаций могут быть ограничения по содержанию информации, передаваемой со служебных телефонов. Такие ограничения (а также ответственность за их нарушение) носят ограниченный (внутрикорпоративный) характер. Единственный случай, когда можно говорить о совершении собеседниками действий, направленных на возникновение у них прав и обязанностей, происходит при обсуждении ими условий сделки с их участием, например, договора купли-продажи. Если по закону не требуется письменной формы для признания действительности такой сделки, можно считать, что в результате телефонного разговора возникло правоотношение, основанное на устном согласии. Но в то же время оно возникает не из-за факта разговора, а из-за характера передаваемой собеседниками друг другу информации.

Подобным образом строятся взаимоотношения клиентов "Интернета" со своими поставщиками, а также между собой. Однако в случае компьютерной, а не телефонной сети, заключение договора между пользователями имеет некоторую специфику. Она заключается в

существенно больших технических возможностях для совершения юридически значимых действий, чем это возможно по телефону или факсу; в способе направления оферты и акцепта; в числе возможных адресатов оферты; в возможностях обсуждения и изменения условий договора; в способе фиксации условий договора в какой-либо материальной форме; в способе исполнения договора лицом, получающим услугу (например, оплачивающим ее производителю). Чаще всего такие вопросы до сих пор остаются не урегулированными национальными правовыми системами.

К тому же подавляющее большинство сделок (не обязательно возмездных) в сети "Интернет" осуществляется между лицами, физически находящимися (либо юридически инкорпорированными) в разных странах, что еще более усложняет ситуацию с определением подлежащего применению права.

Следовательно, уже сейчас можно говорить о специфическом способе (но не основании) возникновения правоотношений между физическими и юридическими лицами, связывающимися между собой посредством компьютерной сети "Интернет". Этот специфический способ:

а) невозможно свести к какой-либо одной из известных форм заключения договоров или возникновения ответственности;

б) связан с использованием исключительно сложного технического оборудования, позволяющего тем не менее обходиться без привлечения специальных познаний для его применения;

в) привлекателен своей оперативностью и удобством применения (в частности, позволяет согласовывать условия сделок и исполнять их в течение нескольких секунд);

г) характеризуется высокой степенью алгоритмизации отношений между субъектами;

д) дает возможность совершать юридически значимые действия, которые направлены на объекты, находящиеся за пределами сферы распространения

национального законодательства. Причем с точки зрения осуществления этот способ значительно проще любого другого.

Последняя характеристика специфики правоотношений, связанных с интернетом, особенно важна при рассмотрении вопроса о нормах, применимых к таким правоотношениям[6].

"Интернет", по крайней мере в настоящий момент, представляет собой интереснейший пример того, насколько удачно и эффективно может развиваться столь сложная техническая система практически в отсутствие формального правого регулирования. Это ставит важный теоретический вопрос о том, как скоро уровень развития социальных отношений, связанный с существованием подобной системы, потребует разработки и применения соответствующего правового регулирования. Следующим, очевидно, будет вопрос о том, насколько эффективным окажется такое регулирование для развития самой технической системы.

В самом деле, до сих пор нормативное регулирование отношений между пользователями, поставщиками и иными участниками "Интернета" не носит правового характера. Помимо многочисленных регламентов и стандартов технического характера к "Интернету" применимы нормы, которые относятся к обычным (традиционным), корпоративным или даже этическим отношениям, разумеется, с соответствующей "интернетовской" спецификой. Это связано с историей возникновения и развития данной сети. На протяжении многих лет она объединяла сравнительно ограниченный круг пользователей из университетских исследовательских центров США. Их отношения (разумеется, не только "сетевые") характеризовались высокой степенью доверительности, уважением к мнению собеседника, определенными правилами вежливости, а также использованием терминологии, хорошо известной собеседникам, но мало понятной людям "со

[6] Наумов А.В. Проблемы совершенствования Уголовного Кодекса Российской Федерации// Государство и право, 1999, №10, с.45; Рузакова О. А., Дмитриев С. С. Авторские и смежные права в Интернете //Законодательство, N 9, сентябрь 2001 – С.32-33

стороны". По мере развития "Интернета" стихийно выработанные, часто нигде не зафиксированные правила "сетевого этикета" (netiquette) становились стандартом поведения и для новых пользователей сети. Сейчас эти правила можно найти в "Интернете" в подробном изложении с комментариями. Конечно, речь не идет об их принудительном применении. В лучшем случае на отступление от правил другие пользователи не обратят внимания (или, наоборот, пошлют гневное замечание), в худшем случае (крайне редко) нарушитель будет частично лишен возможности продолжать общение с другими клиентами.

Чтобы было понятнее, о чем идет речь, приведем следующий пример. Одной из сетевой услуг является так называемый список рассылки, позволяющий получать сообщения по электронной почте на определенные темы от любого пользователя "Интернета", "подписавшегося" на соответствующий список. Существуют правила пользования списками, чаще всего представляющие собой наборы программных команд и алгоритмов, обеспечивающих доступ к информации. Так как эти правила носят чисто технический характер, то их несоблюдение ведет к тому, что неправильно набранная команда не будет исполнена и требуемая информация просто не будет получена. Наряду с техническими правилами имеются и правила "этикета", сходные для всех списков. Например, запрет на рассылку сообщений, не имеющих отношения к установленной теме обсуждения. Также считается недопустимым распространение сообщений коммерческого, рекламного характера в не предназначенных для этого "секторах" сети или подключение к "сетевой начальной странице" без согласия ее владельца.

Нарушение подобных правил не влечет отказа в доступе к передаваемой информации, но может привести к тому, что нарушителю будет сделано замечание в виде посылки сообщения, осуждающего его действия. Причем подобное сообщение может быть послано любым недовольным подписчиком, а их число может достигнуть сотен и даже тысяч. Наконец, нарушитель может быть исключен из списка рассылки, если

решение об этом примет администратор списка. Однако это не означает, что подписчик-нарушитель не сможет вновь стать участником этого же списка (например, под иным именем и адресом) или любого иного списка. Если действия нарушителя "этикета" нельзя признать компьютерным преступлением (к примеру, попыткой взлома системы защиты сервера, с которого происходит рассылка сообщений по списку), то никаких иных, кроме вышеперечисленных, мер наказания к нему применить нельзя. Тем не менее случаи "сетевого хулиганства" достаточно редки. Они широко обсуждаются (и осуждаются) подписчиками "Интернета" в самой сети. В целом же систему правил "сетевого этикета" правомерно охарактеризовать не только как несложную для понимания, запоминания и соблюдения, но и как достаточно эффективную для установления порядка обмена информацией в сети на некоммерческой основе.

Очевидно, именно то, что большинство отношений, возникающих между пользователями "Интернета", по-прежнему не носит коммерческого, возмездного характера и способствует поддержанию относительно высокой эффективности упомянутых норм и правил неюридического характера. При этом можно заметить, что осуществление пользователями в сети определенных действий, часто предельно формализованных, алгоритмизированных, преимущественно направлено на возникновение тех или иных прав и обязанностей у них самих или у их "собеседников". Чаще всего речь идет о способах получения информации, установлении порядка доступа к ней. Уже одно это подчеркивает существенные отличия действий пользователей "Интернета", например, от обмена информацией по телефону. Развитие коммерческих отношений в "Интернете", безусловно, потребует более детальной проработки правил, регулирующих отношения между пользователями сети. Нынешние же нормы поведения участников сетевого общения носят скорее квазиюридический характер. С одной стороны, они применяются в отсутствие какого-либо общесетевого органа централизованного контроля и принуждения. С другой стороны, они

регулируют порядок совершения действий, которые при наличии характеристики возмездности однозначно принято считать имеющими юридическое значение.[7]

О технических нормативных правилах, которые регламентируют порядок объединения различных сетей и необходимые стандарты оборудования и программного обеспечения ("протоколы"), уже вкратце говорилось. Из прочих правил неюридического характера, имеющих отношение к "Интернету", осталось остановиться на корпоративных и формулярных нормах.

Внутрикорпоративные нормы и правила приобретают важное значение в случае присоединения к "Интернету" через узловые компьютеры, установленные в крупных научных центрах и промышленных компаниях. Университеты и корпорации, предоставляющие своим сотрудникам (учащимся) возможность доступа к сети, вправе устанавливать любые правила и ограничения на вход в нее. Подобные ограничения могут носить как чисто количественный (например, временные лимиты), так и качественный характер (например, порядок использования адресов электронной почты, содержащих доменное имя владельца узлового компьютера, или ограничения по передаче конфиденциальных сведений). Политика компаний в данной области достаточно разнообразна и еще ждет своего обобщения.

Исключительно быстро распространяется в "Интернете" практика применения формулярных норм. Благодаря техническим возможностям так называемых средств гиперсвязи (гипертекста) любой пользователь сети может в режиме реального времени сообщить требуемые сведения о себе и желательных для него условиях заключаемой через сеть сделки с применением форм (формуляров), заранее разработанных и размещенных в сети его потенциальным контрагентом. Завершение ввода указанных

[7] Герцева Е. Н. Проблемы квалификации недобросовестного использования доменных имен в Интернете //Законодательство, N 11, ноябрь 2000 – С. 43

сведений, подтверждаемое, например, набором определенной команды или номера кредитной карточки, означает, что сделка заключена. Аналогичная ситуация складывается при заказе товаров по телефону или факсу, когда покупатель фактом устного или письменного сообщения-заказа принимает предложение продавца на его условиях, не подлежащих изменению. Однако в "Интернете" круг возможных сделок несоизмеримо более широк.

В последнее время возникли и применяются даже не просто формулярные контракты "присоединения", в которых одна сторона соглашается с условиями, заранее сообщенными ей второй стороной, но и "формуляры для третьих лиц". Разработано большое количество контрактов со стандартными условиями, которые предлагаются для применения в сетевом режиме. Их заполнение производится либо обеими сторонами одновременно, либо одной из сторон и за себя, и, по поручению другой стороны, за нее. По окончании сеанса договор считается согласованным (заключенным), а фирма-разработчик формулярного контракта получает плату за консультационные услуги (это является одним из стандартных условий).

Применение формулярных договоров и стандартных условий до сих пор не вызывало больших споров. Как правило, такие договоры имеют срочный характер с небольшими сроками исполнения, не связаны с движением значительных денежных сумм и, несмотря на кажущуюся сложность их содержания (это вопрос уже юридической техники), относятся к сравнительно простым правоотношениям. Вряд ли такие формулярные контракты когда-нибудь смогут считаться "полноправным" источником правовых норм, но в настоящее время их применение к соответствующим отношениям достаточно эффективно. Впрочем, в истории права во многих случаях юридическая практика опережала теоретические обоснования создаваемого затем нормативного регулирования.

Итак, отношения между участниками сетевого общения в "Интернете", в том числе и по поводу действий, имеющих юридическое значение,

регулируются неструктурированным массивом нормативных и иных правил. Последние не были установлены в порядке, характерном для принятия правовых актов, и не могут быть принудительно исполнены с использованием возможностей публичной власти. Тем не менее недостаток собственно правовых методов регулирования не помешал стремительному развитию сети в последние годы. Этот феномен еще будет предметом самого внимательного изучения. В ближайшем же будущем развитие в сети отношений, связанных с куплей-продажей товаров и услуг, непременно потребует разработки и применения чисто юридических способов регулирования отношений, защиты интересов пользователей сети (потребителей), пресечения возможности злоупотреблений и правонарушений.

Что касается уже имеющихся нормативных правовых актов, так или иначе затрагивающих отношения по поводу "Интернета", то их можно охарактеризовать следующим образом.

Во-первых, ни в одной из стран мира нет всеобъемлющего (кодифицированного) законодательства по "Интернету". Существующие нормативные (подзаконные) акты регулируют частные аспекты функционирования сети, прежде всего вопросы подключения к ней через поставщиков, предоставления соответствующих линий связи и т.д.

Во-вторых, нормы, которые можно было бы применить к отношениям по поводу "Интернета", "разбросаны" по законодательным актам иных отраслей права. В первую очередь они содержатся в нормах об интеллектуальной и промышленной собственности, а также в разделе, условно именуемом "телекоммуникационным правом". Наибольшую известность получил американский закон "О соблюдении пристойности в средствах связи" (1996), вызвавший оживленную полемику как в "Интернете", так и вне его. Закон предусматривает различные уголовные наказания за размещение в компьютерных сетях и иных средствах связи информации и изображений, "нарушающих приличия", если к такого рода

информации обеспечивается неограниченный доступ. Несмотря на то, что указанный закон рассматривался едва ли не как противоправная попытка введения цензуры в "Интернете", он в целом выполняется владельцами и операторами американских серверов. При этом хорошо известны способы "обхода" установленных запретов - достаточно разместить "нежелательную" информацию на сервере не в США, а, к примеру, на Багамских островах, т.е. вне сферы уголовной юрисдикции США.

В-третьих, практически отсутствует регулирование отношений по поводу "Интернета" на международном (межгосударственном) уровне. Вышеприведенный пример подтверждает, что очень скоро оно потребуется, хотя бы на двусторонней основе[8].

[8] Калятин В.О. Гиперссылки в сети интернет как правовая проблема. //Законодательство, N 10, октябрь 2001 – С. 28

Глава II. Общая характеристика мошенничества с использованием сети Интернет

2.1.Квалификация мошенничества как состава преступления

Мошенничество относится к преступлениям против собственности в виде хищения.

Согласно общим подходам уголовного права, условиями, чтобы преступление против имущества было квалифицировано как хищение, являются:

1. Видовым объектом хищения как преступления выступают отношения собственности как родовое понятие по отношению ко всем формам собственности, а непосредственным объектом выступает та конкретная форма собственности, которая определяется принадлежностью имущества (государственная, частная, муниципальная или собственность общественных объединений).
2. Предметом хищения могут быть вещи и иные предметы материального мира, в создание которых вложен труд человека и которые обладают объективной материальной или духовной ценностью, а также деньги и ценные бумаги, служащие эквивалентом овеществлённого человеческого труда.

Предметом хищения могут быть вещи и иные предметы материального мира, в создание которых вложен труд человека и которые обладают объективной материальной или духовной ценностью, а также деньги и ценные бумаги, служащие эквивалентом овеществлённого человеческого труда.

3. Предметом хищения может быть как движимое, так и недвижимое имущество. Примером хищения недвижимого имущества может быть мошенническое или с применением насилия или угрозы завладение приватизированными квартирами. Объективная сторона хищения

характеризуется активными действиями, выразившимися в противоправном, безвозмездном изъятии и/или обращении чужого имущества в пользу виновного или других лиц и в причинении имущественного ущерба собственнику или иному законному владельцу этого имущества.

Изъятие чужого имущества означает перевод этого имущества из владения собственника или иного законного владельца в фактическое обладание виновного. Обязательный признак хищения – противоправный характер изъятия чужого имущества, т.е. его перевод в фактическое обладание виновного не только без каких-либо законных оснований для этого, но и без согласия собственника или иного законного владельца. Однако изъятие совместного (общего) или спорного имущества либо имущества, в отношении которого изымающий предполагает, хотя и ошибочно, наличие у него определённых прав, не образует состава хищения, но может повлечь ответственность за самоуправство или иные преступления.

Существенным признаком хищения является безвозмездность изъятия чужого имущества. Изъятие считается безвозмездным, если оно проводится без соответствующего возмещения, т.е. бесплатно или с символическим либо неадекватным возмещением. Точно так же является хищением завладение имуществом путём замены его на заведомо менее ценное. Безвозмездность изъятия чужого имущества неразрывно связана с наступлением в результате этого преступления общественно опасных последствий в виде причинения собственнику или иному законному владельцу имущественного ущерба, под которым понимаются прямые убытки, измеренные стоимостью похищенного имущества. Именно с наступлением таких последствий связывается момент окончания хищения. Поэтому хищение чужого имущества должно признаваться оконченным преступлением с момента фактического изъятия имущества, независимо от того, удалось ли виновному распорядиться похищенным имуществом как своим собственным: потребить или использовать иным образом, продать, подарить, передать в долг либо в счёт

уплаты долга и др. Однако для признания хищения оконченным необходимо, чтобы в результате незаконного изъятия чужого имущества виновный получил реальную возможность распорядиться похищенным имуществом по своему усмотрению. Отсутствие такой возможности исключает квалификацию деяния как оконченного преступления.

По общему правилу, как это следует из законодательного определения, хищение состоит из двух элементов: изъятия имущества у собственника или иного законного владельца и обращение его в пользу виновного или других лиц. Однако при таких формах хищения, как присвоение и растрата, хищение имущества происходит без его изъятия, поскольку предмет находится уже в фактическом распоряжении виновного и был вверен ему по различным основаниям (для хранения, управления, транспортировки и т. п.). В такой ситуации хищение состоит из одного элемента – из обращения чужого имущества в пользу виновного или других лиц.

К признакам объективной стороны хищения примыкает причинная связь между противоправными действиями виновного и наступившими общественно опасными последствиями в виде причинения собственнику или иному законному владельцу реального имущественного ущерба.

Субъективная сторона всякого хищения характеризуется виной в виде прямого умысла. Виновный сознаёт общественную опасность своих действий и отсутствие у него всяких прав на похищаемое имущество, предвидит неизбежность наступления вредных последствий в виде причинения собственнику или иному законному владельцу имущественного ущерба и желает их наступления.

К признакам субъективной стороны хищения относятся корыстный мотив и корыстная цель. Сущность корыстного мотива при хищении состоит в побуждениях паразитического характера, в стремлении удовлетворить свои материальные потребности за чужой счёт противоправными способами, путём завладения имуществом, на которое у виновного нет никаких прав.

Корыстная цель при хищении заключается в стремлении получить фактическую возможность владеть, пользоваться и распоряжаться чужим имуществом как своим собственным, т.е. потребить его или лично использовать другим способом, а также продать, подарить или на иных основаниях передать другим лицам. При удовлетворении личных материальных потребностей самого похитителя наличие корыстной цели не вызывает никаких сомнений. Но корыстная цель имеется и в тех случаях, когда похищенное имущество передаётся другим лицам, в обогащении которых виновный заинтересован по различным причинам (при передаче похищенного имущества родным или близким виновного либо лицам, с которыми у него имеются имущественные отношения, например, передача в счёт погашения долга).

Незаконное изъятие чужого имущества без корыстной цели не образует хищения, однако подобные деяния могут квалифицироваться по многим «резервным» статьям УК РФ.

Однако данные признаки характерны для «обычных» хищений – разбоя, грабежа, кражи. Хищения другой группы представляют случаи возможности привлечения к уголовной ответственности тех, кто завладевает чужим имуществом путём **обмана**. Наиболее распространённые виды таких обманных посягательств – мошенничество, а также присвоение и/или растрата вверенного имущества. При этом присвоение и растрату могут совершить только специальные субъекты – материально ответственные лица – и только в отношении вверенного им имущества.

Под мошенничеством закон понимает хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием (ч.1 ст.159 УК РФ). Наказание за это деяние может достигать 3 лет лишения свободы. Более строгая ответственность (вплоть до 6 лет лишения свободы) предусмотрена за мошенничество, совершённое группой лиц по предварительному сговору, либо неоднократно, либо лицом с использованием своего служебного положения, либо с причинением

значительного ущерба гражданину (ч.2 ст.159 УК РФ). И, наконец, за мошенничество, совершённое организованной группой, либо в особо крупном размере, либо лицом, ранее не менее двух раз судимым за хищение или вымогательство (ч.3 ст.159 УК РФ), осуждённый может быть приговорён к лишению свободы на срок от 5 до 10 лет с конфискацией имущества или без таковой.

У С. двоюродный брат попросил взаймы деньги для покупки телевизора. С. дал брату 30 тыс. рублей на два месяца. Но по окончании оговорённого срока брат денег не отдал, пояснив, что месяц назад у него начался запой; одолженные средства, а также премия, из которой он собирался рассчитаться, были истрачены им на спиртное, и возвращать долг ему не из чего.

С. обратился в отделение милиции с просьбой возбудить в отношении родственника уголовное дело о мошенничестве, но в этом ему было отказано.

Дело в том, что для признания действий брата мошенничеством пришлось бы доказать, что С. был введён братом в заблуждение и только под влиянием этого заблуждения передал деньги. Иными словами, милиции необходимо установить, что уже в момент получения денег брат С. не собирался их возвращать, а обещание вернуть было лишь обманом и средством завладения деньгами – иначе пострадавший их бы не дал.

Говоря об основном отличии мошенничества от других форм хищения, Пленум Верховного Суда СССР в Постановлении от 5 сентября 1986 г. № 11 «О судебной практике по делам о преступлениях против личной собственности»[9] указал, что «признаком мошенничества является добровольная передача потерпевшим имущества или права на имущество виновному под влиянием обмана или злоупотребления доверием. Получение имущества под условием выполнения какого-либо обязательства может быть квалифицировано как мошенничество лишь в том случае, когда виновный

[9] См. указанное Постановление

ещё в момент завладения этим имуществом имел цель его присвоения и не намеревался выполнять принятое обязательство».

В рассмотренном случае не вызывает сомнений, что брат С. действительно в момент получения денег собирался покупать телевизор, и лишь когда деньги были даны ему в долг, т.е. законно перешли в его пользование, он решил их не возвращать. Следовательно, обман не был способом получения этих средств, и поэтому мошенничества брат С. не совершал.

В первой части работы речь уже шла о том, что понимается в уголовном праве под имуществом, и рассматривались типичные случаи мошенничества (действия М. – руководителя фирмы, а также карманного вора, вытащившего гардеробный номерок; в последнем случае – покушение на мошенничество). В случае с М. и обманном завладением им безналичными средствами отмечалось: особенностью мошенничества является то, что при этом преступлении можно завладеть не только имуществом, но и правом на него. Ниже приводится именно такой пример.

Некто С. предложил алкоголику Ю., проживавшему в Москве и зарегистрированному (прописанному) в двухкомнатной не приватизированной квартире, обменять её на такую же квартиру за городом с доплатой. Воспользовавшись тем, что Ю. был не в состоянии контролировать происходящее, С. оформил обмен не на квартиру, а на комнату в старой коммунальной квартире.

Таким образом, путём обмана С. стал обладателем квартиры на праве найма. Его обвинили в мошенническом завладении, но не имуществом, а правом пользования жилым помещением.

В этом случае городские власти, которым принадлежит квартира, не понесли ущерба, а поэтому не являются потерпевшими от преступления. Потерпевшим стал несчастный Ю., у которого незаконно, путём обмана, отобрано право пользования жилым помещением.[10]

[10] См. Седугин П. И. Жилищное право М.: 2003 С. 142

Довольно сложны для оценки случаи завладения предъявительской ценной бумагой, по которой имущество похитителем не получено.

Ш. путём обмана получил принадлежащие фирме «Лагуна» облигации внутреннего государственного займа, намереваясь затем их продать Тверьуниверсалбанку. Однако уже на следующий после похищения день жулик был задержан, облигации у него изъяли. Возник вопрос о том, совершено ли оконченное преступление или только покушение на преступление.

Юристы различают **право на ценную бумагу** и **право на бумаги**. Если мы скажем, что Ш. завладел ценными бумагами как имуществом определённой стоимости, мы расценим его действия как оконченное хищение. Такую же оценку заслужат его действия, если мы признаем, что ценная бумага суть право на имущество, и примем во внимание, что уголовно наказуемо мошенничество и в виде незаконного приобретения прав на имущество.

Однако в сходном случае, когда ценные бумаги на предъявителя были украдены, а затем изъяты у вора, следователь посчитал, что хищение не было завершено (окончено), поскольку названные ценные бумаги – лишь право на получение денег, а в статье о краже (в отличие от статьи о мошенничестве) говорится о завладении только имуществом, а не правом на него.

2.2. Основные приёмы мошенничества с использованием Интернета

Роль и значение Интернета в сегодняшней жизни очень велики. Постепенно развиваясь, Интернет перестал быть только средством обмена информацией, а приобрел многофункциональность.

Однако необходимо признать, что Интернет находится в настоящее время в какой-то мере вне законодательного регулирования и контроля государственных органов, что порождает различные правонарушения и

преступления под действием нескольких факторов, которые существенно влияют на криминогенную обстановку, сложившуюся вокруг Интернета.

1. Возможность мошенничества при заключении сделок через Интернет, возможность хищения из виртуальных магазинов, а также создания виртуальных финансовых пирамид.

2. Возможность совершения сделок и операций, скрытых от налоговых органов.

3. Возможность нарушения авторских и патентных прав, а также использования различных информационных баз правоохранительных и контролирующих органов.

4. Возможность совершения преступлений в сфере компьютерной информации (ст.272 УК РФ - неправомерный доступ к компьютерной информации; ст.273 УК РФ - создание, использование и распространение вредоносных программ для ЭВМ, ст.274 УК РФ - нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети).

При мошенничестве в Интернете следует заранее оговориться: Интернет выступает только как средство распространения ложной информации (обмана как обязательного признака мошенничества). Информация в Интернете сама по себе объектом хищения быть не может, так как не является вещью.

Похитить информацию невозможно в юридическом понимании. Вот два примера, которые на первый взгляд можно определить как хищение, правда, как кражу, а не мошенничество:

1.Специалист по ценным бумагам Б., «взломав» компьютерную защиту, установленную начальником кредитного отдела банка, переписал на свою дискету конфиденциальные сведения, чтобы впоследствии продать их конкурентам.

2.Государственный служащий П. тайно вынес из учреждения секретные сведения о разработках новых видов оружия.

Уголовный кодекс РФ указанные деяния не считает хищением, потому что информация не обладает признаком вещественности. Но если информация имеет определённые свойства, то за незаконное завладение ею ответственность всё же предусмотрена, только не статьями УК РФ о хищении, а иными. Например, ст.183 УК РФ устанавливает ответственность за действия, заключающиеся в собирании сведений, составляющих коммерческую или банковскую тайну, путём похищения документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений, составляющих коммерческую или банковскую тайну, без согласия их владельца, совершённые из корыстной или иной личной заинтересованности и причинившие крупный ущерб.

Несколько статей главы 29 УК РФ «Преступления против основ конституционного строя и безопасности государства» охраняют от незаконного «изъятия» информацию, являющуюся государственной тайной (это статьи о государственной измене, шпионаже, разглашении государственной тайны, утрате документов, содержащих государственную тайну).[11]

Об информации прямо говорится в ст.272 УК РФ, где установлено, что за неправомерный доступ к охраняемой законом информации на машинном носителе, в ЭВМ или их сети (т.е. компьютерной информации), если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ или их сети, может назначаться наказание вплоть до лишения свободы до двух лет. А если то же деяние будет совершено 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, то

[11] Основы государства и права /под ред. С.А. Комарова С. 252

виновные могут быть наказаны вплоть до лишения свободы на срок до пяти лет.[12]

Особого рассмотрения заслуживают **безналичные деньги**, т.е. находящиеся на банковских счетах. Очень часто к уголовной ответственности за хищение привлекаются предприниматели, работники банков и прочие граждане, мошеннически завладевшие безналичными денежными средствами. В последнее время получили распространение денежные переводы в Интернете, поэтому следует также определить, можно ли похитить деньги, не имеющие материальной формы? На практике этот вопрос тесно связан с возможностью признания хищения оконченным. Для анализа приводим пример посложнее.

Руководитель фирмы «Снежана» М. заключил договор с фирмой «Дагобар» о поставке сахара. При этом М. не собирался выполнять обязательства по договору и передавать фирме «Дагобар» сахар, а намеревался завладеть авансовым платежом (так называемой предоплатой), который должна была ему передать фирма «Дагобар». Получив на банковский счёт возглавляемой им фирмы указанные средства, М. в течение нескольких рабочих дней размышлял, как использовать эти деньги. Решившись, наконец, «обналичить» их, он был задержан милицией, установившей, что никакого сахара у данной фирмы нет и не было, а аванс её глава, весьма вероятно, собирается похитить. Следователь долго сомневался, похищены ли безналичные деньги (ведь они ещё не были обращены в наличные), или в данной ситуации можно усмотреть лишь покушение на совершение преступления.

Покушение на совершение преступления, как и приготовление к преступлению, - это, согласно уголовному закону, стадии преступной деятельности. В каждой из статей Особенной части УК РФ (с учётом ряда

[12] Копылов В.А. Информационное право. М.: 2002. С. 312

положений его Общей части) содержится описание оконченного преступления. А приготовление к преступлению и покушение на совершение преступления признаются неоконченным преступлением.[13]

Под приготовлением к преступлению понимаются согласно Кодексу: приискание, изготовление или приспособление лицом средств или орудий совершения преступления; приискание соучастников преступления; сговор на совершение преступления либо иное умышленное создание условий для совершения преступления, при этом преступление не было доведено до конца по не зависящим от этого лица обстоятельствам.[14]

Допустим, что В. и А. в пятницу говорили о том, что неплохо бы достать где-нибудь деньги, и решили совершить кражу или иное хищение. В субботу они сделали окончательный выбор в пользу разбойного нападения. В качестве объекта преступления они выбрали инкассаторскую машину Сбербанка, купили два автомата Калашникова, сшили маски и подготовили дачный домик для хранения похищенного. Однако сестра В., узнав об их планах, сообщила в милицию, и сообщники были задержаны ещё до нападения.

Если бы В. и А. были задержаны в пятницу, то им нельзя было бы предъявить обвинение, так как обобщённый, не конкретный разговор не является сговором на совершение преступления. А вот предпринятые ими действия в субботу уже были расценены судом как приготовление к разбойному нападению.

Покушением считаются умышленные действия (бездействие) лица, непосредственно направленные на совершение преступления, если при этом преступление не было доведено до конца по не зависящим от этого лица обстоятельствам.

---

[13] Яни П.С. Преступное посягательство на имущество. // Законодательство. Право для бизнеса, 1998, №9, с.74-75

[14] Основы государства и права /под ред. С.А. Комарова С.256

Описанные стадии и оконченное преступление следует различать. Это может иметь существенное значение, поскольку:

- срок или размер наказания за приготовление к преступлению не может превышать половины максимального срока или размера наиболее строгого вида наказания, предусмотренного соответствующей статьёй за оконченное преступление;
- срок или размер наказания за покушение на преступление не может превышать трёх четвертей максимального срока или размера наиболее строгого вида наказания, предусмотренного соответствующей статьёй за оконченное преступление;
- такие виды наказаний, как смертная казнь и пожизненное лишение свободы за приготовление к преступлению или покушение на преступление вообще не назначаются[15].

В Постановлении Пленума Верховного Суда СССР от 11 июля 1972 г. № 4 «О судебной практике по делам о хищениях государственного и общественного имущества» разъяснено, что «хищение следует считать оконченным, если имущество присвоено, и виновный имеет реальную возможность им распоряжаться по своему усмотрению или пользоваться им».

Теперь можно вернуться к ситуации с безналичными деньгами, которыми хотел завладеть руководитель фирмы «Снежана» М. Согласно ст.128 Гражданского кодекса РФ, к имуществу относятся и деньги. Ст.140 ГК РФ «Деньги» называет рубль платёжным средством, одновременно устанавливая, что платежи на территории Российской Федерации производятся путём наличных и безналичных расчётов. Получается, что так называемые безналичные деньги, т.е. денежные средства, находящиеся на банковских счетах, следует отнести к имуществу, и что их, следовательно, можно похитить. Однако «нематериальность» такого имущества очевидна.

[15] Комментарий к Уголовному кодексу Российской Федерации /под ред. Ю.И. Скуратова и В.М. Лебедева. М.: 1997 – С. 352

Как же решить вопрос: возможно ли хищение безналичных денег, являющихся имуществом, но не имеющих материальной формы?

Дело в том, что хотя банковский вклад и безналичные деньги включаются в понятие «имущество», однако «собственник вклада» и «денежные средства в банковском вкладе» - понятия условные, поскольку и вклад, и безналичные деньги являются правами требования обязательственно-правового, а не вещно-правового характера. И поскольку безналичные деньги – это не вещь, а право требования, то похитить их нельзя. Однако М. не останется безнаказанным, так как ст.159 УК РФ уголовную ответственность не только за хищение имущества, но и за приобретение права на чужое имущество путём обмана или злоупотребления доверием.16 Иначе говоря, М. совершил мошенничество, но не в форме хищения, а в форме завладения имущественным правом путём обмана руководства фирмы-контрагента. Получив на счёт своей фирмы безналичные средства, М. имел возможность в течение нескольких дней, даже не обналичивая, распоряжаться ими по своему усмотрению, поэтому его действия надлежит расценивать не как покушение, а как оконченное преступление.[17]

Рассмотрим теперь случаи мошенничества с использованием Интернета.

Многие на Западе рассматривают в настоящее время переход к электронной коммерции как вопрос жизни и смерти компаний и корпораций. С помощью Интернета некоторые зарубежные компании существенно повысили объемы продаж своей продукции, а те, кто пренебрег всемирной сетью, значительно отстал от конкурентов и им ничего не остается, как просто копировать опыт своих более удачливых коллег.

Метод прямых продаж через Интернет позволяет существенно снизить стоимость продукции, так как отпадает нужда в аренде торговых площадей,

[16] Баяхчев В.Г., Улейчик В.В. Расследование хищений, совершаемых в кредитно-финансовой сфере с использованием электронных средств С. 46

[17] Алексеева Д.Г., Пыхтин С.В., Хоменко Е.Г. «Банковское право» М.: 2004 С. 46

приобретении торгового оборудования, выплаты заработной платы продавцам и иному персоналу.

Торговля через Интернет существенно упрощает жизнь и покупателю. Больше нет необходимости ездить по различным магазинам и ярмаркам в поисках места, где искомый товар стоит дешевле. Стоит лишь провести несколько минут у экрана компьютера, и все цены виртуальных магазинов возникают перед покупателем на мониторе.

К тому же Интернет позволяет производителям продавать свои товары потребителям напрямую, и отпадает необходимость в многочисленных посредниках и перекупщиках.

Электронная торговля быстро развивается. В российской сети каждый день появляются 200 новых сайтов с различными предложениями. По прогнозам специалистов, общий объем рынка Интернет-рекламы достигнет к 2003 году в России 150 млн долл.

Однако Интернет может быть источником опасности. Компьютер занимает большое место в реальном мире, очень многое находится под его управлением. Электронной коммерцией охвачены средний и большой бизнес. Главной проблемой электронной коммерции для юридических лиц является отсутствие в законе системы доказательств, принимаемых и применяемых в судебной практике при рассмотрении споров. Особая проблема - определение места совершенной сделки. А ведь от этого зависят и подсудность, и способы, и размеры налогообложения.

Нынешний уровень законодательной базы не позволяет эффективно решать, когда возникает в этом необходимость, вопросы о месте совершения сделки, месте разрешения спора. Отсутствует ясность, что делать, если по заключенному контракту будет осуществлена оплата продукции и не будет начата ее отгрузка.

При рассмотрении споров, связанных с электронной коммерцией, серьезной помехой является то, что законодательно не определена единая система принимаемых доказательств. Такие споры рассматривает в основном

арбитражный суд. Как показывает практика, в исковых требованиях признать электронную сделку недействительной доказательствами служат электронные и письменные документы, Web-страница, заключение экспертизы".

Специалисты в области правового регулирования сделок в Интернете отмечают опасность, с которой может столкнуться каждый при совершении тех или иных сделок. Естественно, что обширные возможности сети не могут не привлекать тех, кто отдает предпочтение незаконным формам получения прибыли.

Так, в декабре сотрудники милиции по информации службы безопасности интернет-холдинга eHouse задержали гражданина, который с помощью нескольких похищенных за рубежом кредитных карт совершил хищения из магазина Bolero посредством карточки платежной системы WebMoney: сделал около 30 заказов на общую сумму более 15 тыс.долл. Подозрение у менеджеров магазина вызвало большое количество заказов, поступивших от одного человека, за короткий промежуток времени. При первых же фактах, которые подтвердили подозрения, служба безопасности интернет-холдинга передала информацию в правоохранительные органы.

Проблема безопасности интернет-платежей является основной для виртуальных магазинов. Ведь данные специальных карт, предназначенных для оплаты покупок в Интернете, подчас становятся добычей мошенников. Иногда их воруют прямо из баз данных магазинов. А некоторые преступники специально "открывают" виртуальные магазины, реально ничем не торгующие, для сбора информации о картах, предназначенных для безналичных платежей через Интернет. Поэтому для России основным способом платежей остается оплата товара наличными курьеру в момент доставки.

В августе 2000 года сотрудники столичных правоохранительных органов задержали с поличным двух граждан 19 и 27 лет, занимавшихся воровством в российской части сети Интернет реквизитов пользователей карт для

безналичных платежей через Интернет с целью их дальнейшей перепродажи. Хакеры заманивали пользователей сети на свой сайт, предлагая различную интересную информацию. При посещении сайта мошенников пароли считывались вирусом " Троянский конь" и продавались затем с электронного аукциона по демпинговым ценам (по 15 долл., в то время как официальная цена паролей почти в 3 раза выше). По приблизительным подсчетам пользователям был нанесен совокупный ущерб в сумме более 20 тыс. долл.

Из-за развития телекоммуникаций все больше мошенников начинает оперировать в виртуальном пространстве. В 2001 году впервые ущерб от мошенничеств, совершенных с помощью Интернета и электронной почты, впервые превысил ущерб, нанесенный «традиционными» мошенниками, не использовавших компьютер для проведения афер. По данным Центра анализа интернет-мошенничества (Internet Fraud Complaint Center), среднестатистическая жертва интернет-преступления в 2005 году потеряла 1100 евро, жертва «традиционных мошенников» – всего 735 евро.

Лишь 3...5% мошенничеств совершается реальными бизнес-структурами. Мошенники, в большинстве случаев, используют принцип «курочка по зернышку клюет» и наносят своим жертвами относительно небольшой ущерб. В 32% случаев мошенникам удается похитить от 100 до 4500 евро, в 18% – от 1-й до 3-х тыс. евро. Лишь в каждом десятом случае, финансовые потери жертвы превышают 3 тыс. евро Вероятно это происходит и из-за активности правоохранительных органов. Статистика также показывает, что чем крупнее потери ограбленных, с тем большим усердием полиция стремится обнаружить злоумышленника. Большинство мошенников, похитивших суммы более 5 тыс. евро, арестовываются в течение трех-четырех месяцев. Впрочем, несколько лет в розыске находятся мошенники, которые обманом получили от 100 до 1,5 млн. долл.

Действия мошенников не отличаются разнообразием, и они используют лишь несколько широко известных приемов. Однако эти методы работают, несмотря на то, что об опасности подобных действий хорошо

известно. К примеру, некий Марк Броуни (Mark Browne) с 1998 года совершил, как минимум, шесть мошенничеств по одной и той же схеме. Он открывал виртуальный магазин и обзванивал людей с предложениями покупки бытовой электроники по супернизким ценам. Собрав 10...20 тыс. долл., Броуни исчезал.

Статистика показывает, что в США наиболее успешно срабатывают следующие методы завлечения жертв: сообщение, что шанс купить предлагаемую вещь по столь дешевой цене – единственный в жизни; обещание получения денежного приза; обещание, что здоровье человека значительно улучшится; предложение секретной информации, которая позволит жертве заработать и использование запутанных правил, которые потребитель не в состоянии осмыслить. Общаясь с потенциальными жертвами, мошенники обычно подчеркивают, что их деятельность абсолютно законна. Они стремятся использовать названия хорошо известных и солидных фирм (например, для того, чтобы потребитель принял их за сотрудников компании Ivanov & Co, используется название Evanov & Co). Почти в половине случаев, мошенники смогли поймать жертву в свои сети после телефонного разговора.

Наиболее распространённые способы обмана по данным США и стран Евросоюза следующие:

1. Кража информации о кредитных карточках. Мошенники, получившие информацию о личных данных владельца кредитной карточки, могут расплачиваться ею в интернет-магазинах, брать банковские кредиты, арендовать жилье, претендовать на пособия и т.д.
2. Интернет-магазины и аукционы. Схема: покупатель платит деньги за покупку в интернет-магазине, но, либо не получает ее, либо получает товар в меньшем количестве или худшего качества. Наиболее популярный вид жульничества в Интернете. По данным Центра анализа интернет-мошенничества, подобные преступления в 2002 году

составили 27% от числа зафиксированных преступлений во всемирной Сети.

3. Инвестиции Компания предлагает купить ее акции или сделать частные инвестиции, обещая значительную прибыль. Обычно для привлечения жертв, мошенники оперируют фальшивой статистикой и сообщают заведомо ложные сведения об истории или собственниках компании.
4. Сбор пожертвований. Сбор пожертвований широко распространен в США. 90% американцев жертвуют большие или меньшие суммы на различные благотворительные цели. Этим пользуются мошенники. Они просто создают фальшивую благотворительную организацию, которая специализируется на каком-либо добром деле, и совершенно открыто собирают пожертвования. Единственное отличие от обычных благотворительных фондов заключается в том, что деньги прикарманивают мошенники.
5. Восстановление кредитной истории. Практически каждый житель США и каждая компания обладают своей кредитной историей – хроникой получения и погашения кредитов. В США существует несколько независимых кредитных бюро, которые отслеживают кредитную историю американцев, обмениваются информацией и действуют абсолютно независимо как друг от друга, так и от сторонних фирм и организаций. Повлиять на их действия невозможно. Многие американцы оказываются не в состоянии нести кредитное бремя, и их кредитная история ухудшается, что делает невозможным покупку дома, машины и т.д., поскольку банки не хотят связываться с ненадежным заемщиком. Мошенники предлагают за скромную плату «улучшить» кредитную историю – естественно, эти обещания не выполняются, поскольку не могут быть выполнены в принципе.
6. Погашение долгов. Вовремя невозвращенные кредиты и неоплаченные счета считаются личным долгом жителя США. Достаточно часто человек оказывается не в состоянии оплачивать все свои счета. Этим

пользуются мошенники: они предлагают следующую схему: их компания самостоятельно оплачивает счета жителя США и добивается серьезных скидок от кредиторов, а жертва компенсирует затраты компании. В реальности, мошенники лишь получают деньги от своих жертв.

7. Предложение работы. Мошенники предлагают выгодную работу на дому. Однако жертве приходится по грабительским ценам оплачивать предоставляемые расходные материалы, делать гарантийный или вступительный взнос или часть времени работать бесплатно, в качестве испытательного срока.
8. Страховка. «Страховая» компания предлагает рекордно низкие расценки за свои услуги. В действительности, либо эта компания существует лишь на бумаге, либо она закладывает в договор с клиентом такие условия, которые делают невозможным получить страховое возмещение.
9. Льготные кредиты. Физическим лицам часто предлагают льготные кредиты. Однако для получения подобного кредита мошенники требуют сделать некий вступительный взнос (например, чтобы получить кредит в 100 $, жертва платит 150 $) или закладывают в договор грабительские проценты.
10. «Нигерийские письма». Получателю письма предлагается поучаствовать в переводе из нигерийского (ганского, ливийского, конголезского, мозамбикского и т.д.) банка в банк США нескольких миллионов долларов, принадлежащих наследникам африканских президентов, министров, диктаторов, королей и т.д. За свою помощь, получатель должен получить четверть или треть переведенной суммы. Однако, для демонстрации чистоты намерений, жертве предлагается перевести несколько тысяч долларов на счет мошенников. Еще в 2001 году «нигерийским письмам» поверили 15,5% жертв онлайн-

мошенников, в 2002 году количество пострадавших резко упало – до 1%.

11. Финансовые «пирамиды». Данная схема широко известна и впервые была использована несколько сот лет назад. Однако до сих пор финансовые «пирамиды» привлекают жертв. Последняя из рухнувших в США «пирамид» привлекла средства 7 тыс. человек, каждый из которых потерял около 3 тыс. евро
12. Налоги. Иногда жители США не успевают вовремя подать налоговую декларацию. Мошенники предлагают подтасовать данные о времени доставки декларации в налоговые службы и, таким образом, избежать неприятностей.
13. Телефонная связь. Жертве предлагается позвонить по телефонному номеру, где минута разговора стоит огромные деньги. Мелкие телефонные компании также прибегают к мошенничеству: они выставляют своим клиентам счета, куда включены сервисы (например, голосовая почта), которую клиент не заказывал.
14. Туризм. Мошенники или недобросовестные бизнесмены продают своим жертвам туры или билеты в отели, реальные условия в которых значительно уступают рекламе. Например, вместо пятизвездочного отеля жертва мошенников оказывается в трехзвездочном.
15. Революционный метод избавления от излишнего веса. Реклама обещает избавление от лишнего веса в течение дней или недель при использовании нового чудодейственного препарата или диеты. В лучшем случае, жертва станет обладателем бесполезного продукта, в худшем – здоровье окажется под угрозой.

В особенности, мошенничества с использованием Интернета совершаются в связи со специально разобранным выше случаем - безналичными расчётами. Специалисты в области правового регулирования сделок в Интернете отмечают опасность, с которой может столкнуться каждый при совершении тех или иных сделок. Естественно, что обширные

возможности сети не могут не привлекать тех, кто отдает предпочтение незаконным формам получения прибыли.

Так, в августе 2000 года сотрудники столичных правоохранительных органов задержали с поличным двух граждан 19 и 27 лет, занимавшихся воровством в российской части сети Интернет реквизитов пользователей карт для безналичных платежей через Интернет с целью их дальнейшей перепродажи. Хакеры заманивали пользователей сети на свой сайт, предлагая различную интересную информацию. При посещении сайта мошенников пароли считывались вирусом " Троянский конь" и продавались затем с электронного аукциона по демпинговым ценам (по 15 долл., в то время как официальная цена паролей почти в 3 раза выше). По приблизительным подсчетам пользователям был нанесен совокупный ущерб в сумме более 20 тыс. долл.

В декабре 2003 г. сотрудники милиции по информации службы безопасности интернет-холдинга eHouse задержали гражданина, который с помощью нескольких похищенных за рубежом кредитных карт совершил хищения из магазина Bolero посредством карточки платежной системы WebMoney: сделал около 30 заказов на общую сумму более 15 тыс.долл. Подозрение у менеджеров магазина вызвало большое количество заказов, поступивших от одного человека, за короткий промежуток времени. При первых же фактах, которые подтвердили подозрения, служба безопасности интернет-холдинга передала информацию в правоохранительные органы[18].

Проблема безопасности интернет-платежей является основной для виртуальных магазинов. Ведь данные специальных карт, предназначенных для оплаты покупок в Интернете, подчас становятся добычей мошенников. Иногда их воруют прямо из баз данных магазинов. А некоторые преступники специально "открывают" виртуальные магазины, реально ничем не торгующие, для сбора информации о картах, предназначенных для

[18] Баяхчев В.Г., Улейчик В.В. Расследование хищений, совершаемых в кредитно-финансовой сфере с использованием электронных средств. // Законодательство. Право для бизнеса. 2000, №6, с.56

безналичных платежей через Интернет. Поэтому для России основным способом платежей остается оплата товара наличными курьеру в момент доставки.

Также широко мошенничество в Интернете используется при операциях с ценными бумагами. Типичные мошеннические схемы в Интернете по торговле ценными бумагами следующие:

1. Схема "увеличить и сбросить" (Pump&dump) - вид рыночной манипуляции, заключающейся в извлечении прибыли за счет продажи ценных бумаг, спрос на которые был искусственно сформирован. Манипулятор, называясь инсайдером или осведомленным лицом и распространяя зачастую ложную информацию об эмитенте, создает повышенный спрос на определенные ценные бумаги, способствует повышению их цены, затем осуществляет продажу ценных бумаг по завышенным ценам. После совершения подобных манипуляций цена на рынке возвращается к своему исходному уровню, а рядовые инвесторы оказываются в убытке. Данный прием используется в условиях недостатка или отсутствия информации о компании, ценные бумаги которой редко торгуются.

2. Схема финансовой пирамиды (Pyramid Schemes) при инвестировании денежных средств, используя Интернет-технологии, полностью повторяет классическую финансовую пирамиду. При использовании данного приема инвестор получает прибыль исключительно за счет вовлечения в игру новых инвесторов.

3. Схема "надежного" вложения капитала (The "Risk-free" Fraud) заключается в распространении через Интернет инвестиционных предложений с низким уровнем риска и высоким уровнем прибыли. Как правило, эти предложения несуществующих, но очень популярных проектов, таких как вложения в высоколиквидные ценные бумаги банков, телекоммуникационных компаний, в сочетании с безусловными гарантиями возврата вложенного капитала и высокими прибылями.

4. "Экзотические" предложения (Exotic Offerings) - например, распространение через Интернет предложения акций костариканской кокосовой плантации, имеющей контракт с сетью американских универмагов, с банковской гарантией получения через непродолжительный промежуток времени основной суммы инвестиций плюс 15% прибыли.

5. Мошенничества с использованием банков (Prime Bank Fraud) заключаются в том, что мошенники, прикрываясь именами и гарантиями известных и респектабельных финансовых учреждений, предлагают инвесторам вложение денег в ничем не обеспеченные обязательства с нереальными размерами доходности.

6. Навязывание информации (Touting) - часто инвесторов вводят в заблуждение недостоверной информацией об эмитенте, преувеличенными перспективами роста компаний, ценные бумаги которых предлагаются. Недостоверная информация может быть распространена среди широкого круга пользователей сети самыми разнообразными способами: размещена на информационных сайтах, электронных досках объявлений, в инвестиционных форумах, разослана по электронной почте по адресам.

Во избежание потерь средств при инвестировании на иностранных фондовых рынках, инвестору следует придерживаться следующих правил:

1. Осознанно подходить к выбору объекта инвестиций.

Перед тем, как покупать ценные бумаги эмитентов инвестору необходимо ознакомиться с профилем деятельности компании-эмитента, провести историческую оценку движения акций, динамики финансовых показателей эмитента, ознакомиться с последними годовыми и квартальными отчетами, получить информацию о последних корпоративных событиях. В этом смысле полезным источником информации для инвесторов будет сайт раскрытия информации Комиссии по ценным бумагам и биржам США EDGAR (www.sec.gov/edgarhp.htm), а также частные сайты (www.financialweb.com, www.companysleuth.com, www.hoovers.com, www.financewise.com, www.bloomberg.com).

Сравнить кредитный рейтинг интересующего эмитента с рейтингом других эмитентов можно, используя информацию, размещенную на сайтах рейтинговых агентств Moody's и Standard & Poors (www.moodys.com, www.standardpoor.com).

2. Обращаться к услугам брокера, которому доверяете.

Помимо выбора объекта инвестиций инвестор должен определиться в выборе брокерской компании, через которую он намеревается совершить операции. Для того, чтобы избежать возможных недоразумений и убытков, перед открытием счета в брокерской компании целесообразно:

а) выяснить, имеется ли у компании лицензия на осуществление деятельности на рынке ценных бумаг Комиссии по ценным бумагам и биржам США - Securities and Exchange Commission (SEC) (www.sec.gov);

б) узнать о дисциплинарной истории брокерской компании и нарушениях законодательства о ценных бумагах, которые были выявлены у брокерской компании Комиссией по ценным бумагам и биржам США и Национальной ассоциацией дилеров ценных бумаг - National Association of Securities Dealers (NASD). Такую информацию можно найти на сайтах www.sec.gov, www.nasd.com, www.nasdr.com, а также, обратившись в NASD по бесплатному телефону 1-800-289-9999;

в) узнать, является ли брокерская компания членом Корпорации по защите интересов инвесторов в ценные бумаги - Securities Investor Protection Corporation (SIPC), организации, занимающейся разработкой компенсационных схем и выплатой средств инвесторам в случае неплатежеспособности брокерской компании (www.sipc.org).

3. Тщательно обдумывать различного рода "заманчивые" предложения, обещания высоких гарантированных прибылей, избегать контактов с организациями, которые не дают четких и подробных разъяснений в отношении своих инвестиционных механизмов. Брокеры, профессионально работающие на рынке и заботящиеся о своей репутации, заинтересованы в

каждом клиенте и не откажут в предоставлении дополнительной информации о своей компании.

4. Проявлять должную осторожность и осмотрительность при предоставлении информации о паролях доступа к своему инвестиционному счету, номерах банковских счетов, номерах кредитных карт третьим лицам, за исключением случаев, когда есть полная уверенность в том, что получатель информации действует на законных основаниях и ее раскрытие действительно необходимо для совершения сделки.

5. Использовать лимитные приказы во избежание покупки или продажи акций по ценам выше или ниже желаемой. Лимитный приказ на покупку или продажу ценных бумаг предполагает наличие заранее определенной инвестором цены исполнения. В случае размещения рыночного приказа у инвестора отсутствует контроль за ценой исполнения приказа. Брокер может злоупотребить незнанием инвестора относительно цен, сложившихся на рынке, что может привести к непредвиденным финансовым потерям для инвестора.[19]

Анонимность, которую предоставляет своим пользователям сеть Интернет, возможность охвата большой аудитории, высокая скорость и гораздо более низкая стоимость распространения информации по сравнению с традиционными средствами, делает Интернет наиболее удобным инструментом для мошеннических действий.

В связи с этим особо актуальной становится проблема борьбы с мошенничеством и иными компьютерными преступлениями, и эта борьба должна осуществляться на двух уровнях – национальном и международном.

[19] Безверхое А.Г. Собственность и имущественные отношения в уголовном праве. //Законодательство. Право для бизнеса. 2002, №12, с.52

Глава III. Перспективы борьбы с мошенничеством в Интернете

3.1.Проблемы оперативно-розыскной деятельности в связи с преступлениями с использованием сети Интернет

Проблема борьбы с преступностью в Интернете, в том числе и с мошенничеством, относится, прежде всего, к области совершенствования нормативно-правового регулирования деятельности правоохранительных органов, а также к работам криминалистического и криминологического характера. В общегосударственном масштабе были разработаны некоторые профилактические меры. К числу значимых можно с уверенностью отнести изменения в уголовном законодательстве ещё при принятии нового Уголовного кодекса России (1996), в результате чего криминализированы (т.е. признаны преступными, уголовно наказуемыми) определенные деяния в сфере компьютерной информации, имеющие повышенную общественную опасность.

В частности, нормы о преступлениях в означенной сфере зафиксированы в трех статьях Уголовного кодекса Российской Федерации (УК РФ): ст.272 (Неправомерный доступ к компьютерной информации), ст.273 (Создание, использование и распространение вредоносных программ для ЭВМ) и ст.274 (Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети). Общим объектом названных преступлений являются общественные отношения в сфере обеспечения информационной безопасности, а к непосредственным объектам преступного посягательства относятся базы и банки данных конкретных компьютерных систем или сетей, их отдельные файлы, а также компьютерные технологии и программные средства их обеспечения, включая средства защиты компьютерной информации.

Таким образом, своевременный прогноз позволил не допустить резкого негативного изменения криминальной ситуации: компетентные государственные органы были готовы нейтрализовать проявления новых видов преступности, а своевременно информированные руководители организаций и

предприятий различных форм собственности, а также частные лица в большинстве своем не стали жертвами преступлений.

Следовательно, даже не очень точное, предположительное знание лучше полного неведения. Поэтому представляется полезным уже сейчас определить с криминологической точки зрения перспективы дальнейшей компьютеризации и информатизации российского общества. Представляется, что со временем в сфере компьютерных сетей, в том числе глобальных с большой вероятностью можно ожидать увеличения числа правонарушений. И если уже сейчас не начать самым активным образом бороться с криминализацией Интернета, то в недалеком будущем нам придется пожинать горькие плоды своей беспечности. Чтобы оценить криминогенный потенциал "всемирной паутины", достаточно просмотреть Уголовный кодекс. По сути, посредством эксплуатации возможностей сети могут совершаться самые разнообразные преступления.

Для удобства изложения материала все предусмотренные Особенной частью УК РФ составы преступлений условно разделим на две группы:

а) деяния, совершение которых с помощью компьютерных сетей теоретически возможно;

б) 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 компьютерных сетей, 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. Некоторые хакеры утверждают, что им под силу все кроме изнасилования.

Таким образом, в рассматриваемых условиях вполне может быть совершена значительная часть уголовно наказуемых деяний. Прежде всего, это

преступления, которые уже выявляются и пресекаются правоохранительными органами. К их числу помимо упомянутых чисто "компьютерных" (ст.272 - 274 УК РФ) относятся преступления против собственности кража (ст.158 УК РФ) и мошенничество (ст.159 УК РФ).

Однако даже небольшое путешествие по Интернету позволяет с полной уверенностью предположить, что помимо выявляемых уголовно наказуемых деяний посредством сети уже сейчас совершается немало других преступлений. В эту группу входят те составы, признаки которых при желании могут быть обнаружены в Интернете. В частности, это клевета (ст.129 УК РФ), оскорбление (ст.130 УК РФ), нарушение неприкосновенности частной жизни (ст.137 УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст.138 УК РФ), нарушение авторских и смежных прав (ст.146 УК РФ), нарушение изобретательских и патентных прав (ст.147 УК РФ), незаконное предпринимательство (ст.171 УК РФ), заведомо ложная реклама (ст.182 УК РФ), незаконное распространение порнографических материалов или предметов (ст.242 УК РФ), возбуждение национальной, расовой или религиозной вражды (ст.282 УК РФ) и др.

Наконец, вероятно использование злоумышленниками всемирной компьютерной сети для обмана потребителей (ст.200 УК РФ) и незаконного получения и разглашения сведений, составляющих коммерческую или банковскую тайну (ст.183 УК РФ). Кроме прочего, Интернет может служить (и скорее всего, уже служит) инструментом для шпионажа (ст.276 УК РФ) и других преступлений против государственной власти и т.п.

Характеристику криминального потенциала электронно-вычислительных систем и их сетей можно продолжать, но не это главное. Знание проблемы, понимание опасности - не самоцель. Суть проблемы заключается в том, чтобы понять, каким образом предотвратить дальнейшую криминализацию Интернета.

По сути, Интернет в настоящий момент полностью неуправляем. Хотя, по мнению многих, такая неуправляемость - признак свободы. В принципе любая организация, любое частное лицо, используя стандартный набор программно-

технических средств, имеет возможность эксплуатировать потенциал всемирной сети.

Правоохранительная деятельность отечественных государственных структур здесь малозаметна. Пользователи сети руководствуются своими писаными и неписаными правилами поведения, но далеко не все они готовы добровольно соблюдать правовые нормы. Преступники же находят все новые и новые возможности применения своих криминальных способностей в Интернете, и они не должны оставаться безнаказанными. Актуальность проблемы подтверждают относительно недавние события: руководители бандитских формирований, действовавших на территории Дагестана, распространяли свои приказы посредством сети Интернет.

Важно, чтобы правоохранительные органы государства были не просто готовы к нейтрализации обозначенного негативного потенциала сети, но и чтобы они заняли в этом вопросе активную позицию. В частности, хотелось бы, чтобы они проявляли большую активность в сфере профилактики и выявления преступлений, совершаемых посредством сетей Интернет.

Тот факт, что по перечисленным ранее составам преступлений пока крайне редко возбуждаются уголовные дела, вполне объясним. Уголовно-процессуальным законодательством определен ограниченный круг субъектов, уполномоченных принимать процессуальное решение о возбуждении уголовного дела. К их числу относятся суд (судья), прокурор, следователь и орган дознания. В свою очередь, названные субъекты должны всесторонне и тщательно оценить поводы и основания, прежде чем вынести постановление о возбуждении уголовного дела. В соответствии с УПК РФ поводами к возбуждению уголовного дела являются:

а) заявления и письма граждан;

б) сообщения общественных организаций;

в) сообщения предприятий, учреждений, организаций и должностных лиц;

г) статьи, заметки и письма, опубликованные в печати;

д) явка с повинной;

е) непосредственное обнаружение органом дознания, следователем, прокурором или судом признаков преступления.

Однако многие наши граждане обычно избегают решительных действий при обнаружении признаков преступлений. Руководители предприятий, учреждений, общественных организаций не желают лишний раз общаться с сотрудниками правоохранительных органов. Сами преступники вряд ли стройными рядами пойдут в милицию. Таким образом, единственным реальным в настоящее время поводом для возбуждения уголовного дела по факту совершения преступления в глобальной компьютерной сети является непосредственное обнаружение последнего компетентными должностными лицами. С учетом нищенского положения наших правоохранительных органов, когда во многих районах даже центральных городов следователи и сотрудники дознания еще не используют компьютеры в работе, ожидать их активной борьбы с преступлениями, совершенными посредством Интернета, преждевременно. Эту ситуацию вряд ли исправит в ближайшее время и созданное около года назад в системе МВД специализированное подразделение.

Имеются и другие факторы, повышающие латентность рассматриваемой категории преступлений. К примеру, многие фирмы во избежание антирекламы предпочитают не предавать гласности случаи посягательств на их интересы.

Таким образом, без усиления контроля со стороны уполномоченных органов государства не обойтись. Однако идея контроля со стороны спецслужб за пользователями всемирной компьютерной сети Интернет встречает много противников. На страницах специализированных изданий идут жаркие дискуссии о потенциальном вреде подобного контроля и даже обсуждаются возможные методы борьбы с ним.

Так уж исторически сложилось в нашем государстве, что к деятельности сыскных ведомств люди относятся, мягко говоря, неоднозначно. С одной стороны, эта специфическая и небезопасная деятельность окружена ореолом героической таинственности, а люди, к ней причастные, пользуются заслуженным авторитетом. И для этого есть все основания.

Но есть и другая, оборотная сторона медали. Являясь достаточно эффективным средством ограждения интересов личности, общества и государства от преступных посягательств, оперативно-розыскная деятельность в определенных условиях может превратиться в свой антипод - инструмент насилия и произвола, и это уже случалось в определенные периоды российской истории и перед Октябрьской революцией, и во времена "культа личности". В печати приводилось достаточно примеров всевозможных злоупотреблений тех лет, поэтому нет необходимости углубляться в эту тему.

Таким образом, при определенных условиях оперативно-розыскная деятельность, призванная защищать от преступных посягательств жизнь, здоровье, права и свободы человека и гражданина, его собственность, служить обеспечению безопасности общества и государства, может быть использована в противоположных целях.

Поэтому понятна позиция противников контроля со стороны государства за пользователями сети они небезосновательно опасаются возможных злоупотреблений. Кроме того, просто неприятно знать, что за тобой могут следить. И все же иного выхода, очевидно, пока действительно нет. Без активизации работы сыскных ведомств остановить рост преступных проявлений в сети Интернет невозможно. Но как обеспечить надежную защиту охраняемых уголовным законом общественных отношений и при этом не допустить злоупотреблений, ущемляющих права пользователей сети?

Вопрос сложный, но, тем не менее, требующий ответа. Представляется, что при условии соблюдения спецслужбами норм Конституции, уголовно-процессуального законодательства и иных законов, действующих в данной сфере, права пользователей сети нарушены не будут. До недавнего времени деятельность оперативно-розыскных органов не была законодательно урегулирована. Именно тот факт, что оперативно-розыскные службы органов внутренних дел и государственной безопасности долго руководствовались не законом, а ведомственными приказами и инструкциями, совершенно справедливо расценивался многими правоведами как негативный. Вся оперативно-розыскная деятельность была до такой степени засекречена, что

доступа к ней не имели ни прокуроры, ни судьи. Подобная закрытость кроме положительных сторон имела и отрицательные, так как приводила порой к бесконтрольности и соответственно к нарушениям закона, ограничениям прав и законных интересов граждан.

В условиях построения правового государства такое положение долго сохраняться не могло. И в 1992 г. деятельность органов, применяющих оперативно-розыскные средства, впервые в истории России была урегулирована законом "Об оперативно-розыскной деятельности в Российской Федерации", в настоящее время утратившим силу. Развивая его положения, ныне действующий акт предусматривает стройную систему контроля органов государственной власти и управления, а также прокурорский надзор за законностью деятельности оперативно-розыскных органов.

В соответствии со ст. 20 действующего Федерального закона от 12 августа 1995 г. N 144-ФЗ "Об оперативно-розыскной деятельности" контроль за оперативно-розыскной деятельностью осуществляют Президент Российской Федерации, Федеральное Собрание Российской Федерации, Правительство Российской Федерации в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

Статья 1 (ч.2) Закона РФ "О прокуратуре Российской Федерации" предусматривает, что в целях обеспечения верховенства закона, единства и укрепления законности, защиты прав и свобод человека и гражданина, а также охраняемых законом интересов общества и государства прокуратура Российской Федерации осуществляет в числе прочего:

а) надзор за соблюдением прав и свобод человека и гражданина федеральными министерствами и ведомствами, представительными (законодательными) и исполнительными органами субъектов Российской Федерации, органами местного самоуправления, органами военного управления, органами контроля, их должностными лицами, а также органами управления и руководителями коммерческих и некоммерческих организаций;

б) надзор за исполнением законов органами, осуществляющими оперативно-розыскную деятельность, дознание и предварительное следствие.

Огромную роль в обеспечении соблюдения конституционных прав и свобод в сфере оперативно-розыскной деятельности играет также судебный контроль. Однако мы не будем здесь подробно рассматривать всю контрольно-надзорную систему, призванную наблюдать за деятельностью спецслужб. Более важно дать хотя бы краткую характеристику прав граждан, вольно или невольно вовлеченных в сферу оперативно-розыскной деятельности правоохранительных органов.

Всякое необоснованное ущемление предоставленных Конституцией прав и свобод дает гражданину основание воспользоваться принадлежащим ему правом обжалования незаконных действий должностных лиц государства. Именно активная позиция самих граждан, чьи интересы неправомерно ущемляются, позволяет эффективно действовать упомянутой контрольно-надзорной системе государства.

Обжалование действий оперативно-розыскных служб осуществляется в соответствии с ч.3 ст.5 закона "Об оперативно-розыскной деятельности", в которой сказано следующее: "Лицо, полагающее, что действия органов, осуществляющих оперативно-розыскную деятельность, привели к нарушению его прав и свобод, вправе обжаловать эти действия в вышестоящий орган, осуществляющий оперативно-розыскную деятельность, прокурору или в суд".

Таким образом, заинтересованное лицо самостоятельно выбирает адресата, к которому считает целесообразным обратиться за защитой своих прав. В свою очередь, вышестоящий орган, прокурор либо судья при нарушении органом (должностным лицом), осуществляющим оперативно-розыскную деятельность, прав и законных интересов физических и юридических лиц в соответствии с законодательством Российской Федерации обязан принять меры к восстановлению этих прав и законных интересов, возмещению причиненного вреда.

Предметом обжалования может быть незаконное осуществление любого из оперативно-розыскных мероприятий, которые перечислены в ст.6 закона "Об

оперативно-розыскной деятельности". К ним относятся: опрос; наведение справок; сбор образцов для сравнительного исследования; проверочная закупка; исследование предметов и документов; наблюдение; отождествление личности; обследование помещений, зданий, сооружений, участков местности и транспортных средств; контролирование почтовых отправлений, телеграфных и иных сообщений; прослушивание телефонных переговоров; снятие информации с технических каналов связи; оперативное внедрение; контролируемая поставка; оперативный эксперимент.

Перечисленные действия считаются проведенными с нарушением в том случае, когда соответствующие органы (должностные лица) при проведении указанных мероприятий не обеспечили соблюдение прав человека и гражданина на неприкосновенность частной жизни, личную и семейную тайну, неприкосновенность жилища и тайну корреспонденции. Недопустимым считается также осуществление оперативно-розыскной деятельности для достижения целей и решения задач, не предусмотренных законом "Об оперативно-розыскной деятельности".

Согласно ст.5 названного акта, органам (должностным лицам), осуществляющим оперативно-розыскную деятельность, также запрещается:

а) проводить оперативно-розыскные мероприятия в интересах какой-либо политической партии, общественного и религиозного объединения;

б) принимать негласное участие в работе федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, а также в деятельности зарегистрированных в установленном порядке и не запрещенных политических партий, общественных и религиозных объединений в целях оказания влияния на характер их деятельности;

в) разглашать сведения, которые затрагивают неприкосновенность частной жизни, личную и семейную тайну, честь и доброе имя граждан и которые стали известными в процессе проведения оперативно-розыскных мероприятий, без согласия граждан, за исключением случаев, предусмотренных федеральными законами.

Однако вернемся к вопросу о соблюдении закона "Об оперативно-розыскной деятельности" при осуществлении оперативно-розыскной деятельности в конкретной сфере - применительно к глобальной компьютерной сети Интернет. Очевидно, что использование положений этого документа в столь специфической среде имеет особенности. Это надо учитывать при определении законности и обоснованности действий должностных лиц, осуществляющих оперативно-розыскную деятельность.

Само по себе использование средств компьютерной связи, да и в целом телекоммуникационных систем в оперативно-розыскных целях допустимо. Так, часть 3 ст. 6 закона "Об оперативно-розыскной деятельности" гласит: "В ходе проведения оперативно-розыскных мероприятий используются информационные системы, видео-, аудиозапись, кино- и фотосъемка, а также другие технические средства и иные средства, не причиняющие вреда жизни и здоровью личности и окружающей среде". Таким образом, законодатель не ограничивает оперативно-розыскные органы в применении различных технических средств. Главное условие, поставленное законодателем, заключается в том, чтобы их использование не влекло угрозы жизни и здоровью людей и не причиняло вреда окружающей среде.

Какие же из указанных в рассматриваемом законе оперативно-розыскных мероприятий могут проводиться в сетях Интернет*(4)? Анализ главы II этого акта позволяет сделать вывод о том, что к таковым относятся: опрос граждан; наведение справок; сбор образцов для сравнительного исследования; проверочные закупки; наблюдение; контролирование почтовых отправлений, телеграфных и иных сообщений; снятие информации с технических каналов связи. И если такие мероприятия, как, например, опрос и наведение справок ни в коей мере не ограничивают конституционного статуса личности*(5), то контроль за сообщениями и снятие информации с технических каналов связи непосредственно затрагивают конституционные права граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

Разумеется, всегда остается вероятность того, что должностные лица спецслужб государства могут допустить злоупотребления. Однако подобной опасностью чревата почти каждая специальная мера, применяемая для борьбы с преступностью. Тем более в силу того, что практика противодействия распространению преступности в компьютерных сетях только начинает нарабатываться, обеспечение гарантий в рассматриваемой сфере все еще имеет неопределенный характер. В этой связи для недопущения необоснованного ущемления прав пользователей сети представляется недостаточным наличия лишь правовых гарантий. Полезным было бы увеличение числа независимых квалифицированных экспертов, которые могли бы (пусть даже на коммерческой основе) оказывать помощь тем пользователям сети (физическим и юридическим лицам), которые считают себя жертвами обозначенных злоупотреблений*(6).

В завершение этого обобщенного, а потому недостаточно полного рассмотрения некоторых проблем, касающихся возможного вмешательства в жизнь пользователей Интернет органов, осуществляющих оперативно-розыскную деятельность, рассмотрим еще один аспект проблемы.

Законом "Об оперативно-розыскной деятельности" особо выделяется категория лиц, виновность которых в совершении преступления не доказана в установленном законом порядке. Имеются в виду лица, в отношении которых в возбуждении уголовного дела отказано либо уголовное дело прекращено в связи с отсутствием события преступления или в связи с отсутствием в деянии состава преступления. Если такое лицо располагает фактами о проведении в отношении него оперативно-розыскных мероприятий (в том числе посредством сети Интернет) и полагает, что при этом были нарушены его права, оно вправе истребовать от органа, осуществляющего оперативно-розыскную деятельность, сведения о полученной о нем информации в пределах, допускаемых требованиями конспирации и исключающих возможность разглашения государственной тайны. Если в предоставлении запрошенных сведений будет отказано или если указанное лицо полагает, что сведения получены не в полном объеме, оно вправе обжаловать действия такого органа в судебном порядке. В процессе рассмотрения дела в суде обязанность доказывать обоснованность

отказа в предоставлении этому лицу сведений, в том числе в полном объеме, возлагается на соответствующий орган, осуществляющий оперативно-розыскную деятельность.

В целях обеспечения полноты и всесторонности рассмотрения дела указанный орган обязан предоставить судье по его требованию оперативно-служебные документы, содержащие информацию о сведениях, в предоставлении которых было отказано заявителю, за исключением сведений о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, и о лицах, оказывающих им содействие на конфиденциальной основе.

В случае признания необоснованным решения органа, осуществляющего оперативно-розыскную деятельность, об отказе в предоставлении необходимых сведений заявителю судья может обязать указанный орган предоставить заявителю соответствующие сведения.

Таким образом, российское законодательство сейчас позволяет не только компетентным органам и должностным лицам, но и гражданам контролировать соблюдение законности при проведении негласной работы. Хочется верить, что даже с учетом некоторого несовершенства законодательства подобная открытость позволит укрепить доверие пользователей компьютерных сетей к соответствующим ведомствам правоохранительных органов, что даст возможность навести порядок в киберпространстве.[20]

3.2. Международно-правовое сотрудничество по борьбе с мошенничеством в Интернете

Наряду с совершенствованием законодательной базы на национальном уровне важным аспектом выступает международно-правовой, так как сеть Интернет носит всемирный характер. Правоохранительные органы какого государства должны содействовать принудительному исполнению судебного

[20] Голубев В. В. Интернет и оперативно-розыскная деятельность //Законодательство, 1999, N 11 – С.21

решения, если оно все-таки будет вынесено? Ясных ответов на все эти вопросы нет, хотя определенные подходы к их решению просматриваются.

Применительно к уголовному (и административному) праву обсуждался закон канадской провинции Британская Колумбия, запрещающий жителям провинции размещать в средствах связи и массовой информации объявления с предложением взять приемного ребенка. Распространяется ли юрисдикция указанной провинции на размещение таких объявлений в "Интернете" через серверы, расположенные в других провинциях Канады или других странах мира? Основная проблема заключается в том, что "Интернет", не имея территориальных границ своего распространения, позволяет любому жителю провинции получить доступ к информации, распространение которой каким-либо иным способом прямо запрещается.

Оптимальным решением указанных проблем стала бы как можно более полная унификация национальных и региональных законодательств. Поскольку в обозримом будущем такая унификация явно невозможна, "Интернет" даст дополнительный импульс процессу гармонизации, сближения национальных правовых систем (хотя бы в части, призванной регулировать отношения в самой сети).[21]

При выходе на потенциального контрагента в "Интернете" чаще всего используются "сетевые начальные страницы", соединенные между собой так называемыми связями гипертекста, облегчающими поиск нужной информации, товара или услуги.

Однако владелец "начальной страницы" (точнее, "участка сети", на котором она размещена) не обязательно является одновременно ее администратором (тем, кто реально занимается обработкой данных, проходящих через "страницу", и обеспечением ее размещения в сети). Подчас с помощью "начальной страницы" производится только выход на совершенно иной сервер, где запрошенная услуга может быть реально оказана. Наконец, чаще всего владельцы "участков" не являются владельцами или администраторами тех серверов, где размещены их "страницы" и доменные имена которых являются

[21] Иванов Н.Г. Принцип субъективного вменения и его реализация в УК РФ.// Государство и право, 1999, №10, с.57

частью адреса такой страницы. В результате бывают случаи, когда пользователь сети, обратившийся за оказанием какой-либо услуги на определенный сервер и определенную "начальную страницу", достоверно не информируется о полномочиях лица, который осуществляет с ним обмен информацией. Кроме того, такой обмен может производиться не человеком, а компьютерной программой. Вследствие этого заключенную сделку в принципе можно оспаривать по основаниям ultra vires. Для предотвращения таких ситуаций целесообразно было бы создать механизм достоверной идентификации субъекта предлагаемого правоотношения, при котором ответственность за достоверность возлагалась бы на лицо, предлагающее сетевую услугу. Можно было бы, к примеру, установить правило, согласно которому по умолчании (если прямо не заявлено иное) продавцом услуги (товара, информации) всегда будет владелец "сетевого участка".

Схожие проблемы возникают при определении полномочий собеседника, с которым производится обмен сообщениями по электронной почте. Как уже отмечалось выше, корпоративные правила доступа сотрудников к электронной почте могут значительно различаться, и по крайней мере в будущем была бы желательна унификация (правовая регламентация) их наиболее существенных положений.

Одной из правовых проблем идентификации пользователей "Интернета" в более широком смысле является вопрос об "адресах". У каждого компьютера всегда два адреса. Один из них (числовой адрес), предназначенный для связи компьютеров между собой, состоит из четырех чисел и практически не применяется пользователями. Второй адрес - узловое имя, состоящее из компонента, указывающего на местоположение или тип организации, владеющей компьютером, и из доменного имени. Доменное имя должно быть уникальным и всегда принадлежит только одному лицу (или организации). Любое лицо или организация могут иметь одновременно несколько разных доменных имен.

Регистрацией доменных имен занимается организация под названием Центр сетевой информации ("ИнтерНИК"). До 1994 г. "ИнтерНИК"

регистрировал доменные имена в заявительном порядке, без проверки наличия у претендента прав на данное наименование. В результате значительное число доменных имен, совпадающих с широко известными и зарегистрированными фирменными наименованиями (торговыми именами) оказалось у пользователей сети, не имевших отношения к владельцам торговых имен. Типичный пример: доменное имя "coke.com", совпадающее с торговым именем "coke", которое принадлежит известной компании "Кока-кола", оказалось заблаговременно зарегистрированным частным лицом из штата Калифорния.

Заключение возмездных сделок через "Интернет" требует диверсификации способов оплаты таких сделок и влечет за собой усложнение правоотношений по поводу производимых расчетов. Это происходит как за счет увеличения способов безналичных расчетов, так и за счет вовлечения в процесс расчетов новых, чисто "сетевых" субъектов ("виртуальных банков").

Наряду с традиционными способами безналичной оплаты (банковский перевод, банковский чек, кредитная или дебетная карточка) стали применяться "телефонные деньги" (лицо, пользующееся сетевой услугой, соглашается на включение платы за нее в счет, выставляемый ему за пользование "Интернетом" в целом). Как уже говорилось, наиболее распространена оплата услуг поставщика сети, сходная с абонентской платой за телефон. Таким образом, в процесс расчетов вовлекаются по крайней мере два новых субъекта (помимо плательщика и получателя платежа): поставщик "Интернета" и местная телефонная компания. Налицо множественность субъектного состава обязательства, требующая серьезного юридического оформления всех "внутренних" и "внешних" правоотношений, носящих договорный характер.

Появилось и совершенно новое понятие - "электронные наличные" (или "электронные деньги"), которые представляют собой условные расчетные единицы, эквивалентные количеству "реальных" денег на счету пользователя в процессинговой компании ("виртуальном банке"), осуществляющей расчеты по сделке. Такой способ исключительно оперативен (занимает до нескольких минут). Однако он применим только к сделкам, заключаемым в сети. При

оформлении отношений пользователя с "виртуальными банками" особенно широко применяются формулярные контракты.

Остаются пока открытыми вопросы о том, какие минимальные требования должны предъявляться к "виртуальным банкам", каковы условия и пределы их ответственности. Представляется, что общие требования к организациям, производящим сетевые расчеты, не должны существенно отличаться от предъявляемых к "несетевым" расчетно-кредитным учреждениям и должны быть закреплены в соответствующих нормативно-правовых актах. Отношения по поводу сетевых расчетов имеют ту же сущность, что и по поводу денежных расчетов вообще, и их специфика связана не с содержательной стороной, а лишь с формой реализации таких отношений сторонами.

При анализе расчетных отношений в сети нельзя не затронуть вопрос о безопасности передачи данных, содержащих конфиденциальную информацию, в более общем плане. Обеспечивает ли "Интернет" сохранение тайны личной переписки через электронную почту; можно ли скопировать информацию, не предназначенную для передачи третьим лицам; защищена ли информация, передаваемая по сети, от компьютерных вирусов? Пока большинство экспертов дает неутешительный ответ: "Интернет" не обеспечивает желательного уровня безопасности. Причем это связано даже не столько с отсутствием необходимых технических возможностей, сколько с политикой компаний, предоставляющих сетевые услуги. Можно внедрить уровни защиты, для "взлома" которых потребуются такие затраты средств и рабочего времени, что они станут просто невыгодными для недобросовестного пользователя сети. Но при этом уменьшатся и удобства для добросовестных клиентов (потребуется запоминать много дополнительной информации, например, паролей; возможно, потребуется приобрести дополнительное оборудование), что снизит для некоторых из них привлекательность оказываемой услуги и побудит обратиться к конкурентам.

Иным методом обеспечения конфиденциальности является применение средств шифрования. Это непосредственно затрагивает интересы государственной безопасности, и США, например, ограничивают пределы применения средств шифрования при передаче информации через сеть. Особо

жестко регулируется (по существу, запрещается) передача и экспорт собственно шифровальных средств - компьютерных программ и аппаратного обеспечения. Возникает коллизия между интересами государства и частного пользователя. Она имеет как теоретический интерес - соответствуют ли вводимые ограничения конституционным правам на свободу слова (в более узком значении - на передачу информации), так и практическое значение для охраны имущественных и иных законных интересов пользователей сети при совершении возмездных сделок.

Одним из самых распространенных способов финансового мошенничества в Интернете является привлечение средств инвесторов при первичном размещении акций (IPO). В этом случае злоумышленники привлекают инвесторов обещаниями легкой и быстрой прибыли, получаемой при развитии частных компаний так называемой новой экономики.

Интернет в принципе предоставляет неплохую возможность для ведения безнаказанной мошеннической деятельности. Однако изобрести безупречную схему получения денег, добытых этим путем, достаточно трудно. Большинство мошенников попадаются именно на этом этапе.

Хотя виртуальные деньги уже появились, без возможности потратить их на что-то реальное, они не представляют никакой ценности. Это изменится только тогда, когда виртуальное выпивание бутылки пива будет приносить реальное удовлетворение. Заслуживает упоминания еще один немаловажный аспект специфики правоотношений, возникающих по поводу "Интернета" - вопрос доказывания фактов, имеющих юридическое значение.[22]

Производимые пользователями сети операции с информацией (ввод данных, их перезапись, копирование и обработка) подобны составлению письменных документов и их рассылке. Однако, в отличие от письменных документов на бумажном носителе, информация, циркулирующая в сети, не может быть так же легко предъявлена для считывания и изучения. По крайней мере требуется специальное оборудование (компьютер), чтобы указанную информацию получить из сети для непосредственного восприятия и

[22] Калятин В.О. Гиперссылки в сети интернет как правовая проблема. //Законодательство, N 10, октябрь 2001 – С. 33

осмысления. Вопрос о признании документов на магнитных и аналогичных носителях в качестве письменных доказательств неоднозначно решается в разных правовых системах. Развитие "Интернета" пока только усложняет решение о допущении циркулирующей в сети информации в качестве доказательств, хотя и делает этот вопрос чрезвычайно актуальным. В самом деле, на что должен ссылаться пользователь "Интернета", потерпевший убытки вследствие ненадлежащего исполнения обязательств фирмой - производителем сетевых услуг, если договор с ней был заключен в виде обмена информацией через "начальные страницы" этой фирмы, размещенные на ее "сетевом участке"? Как доказываются условия заключенной сделки (хотя бы намерения сторон), если фирма может в любой момент изменить условия формулярного контракта? (Текст формулярного контракта на момент подачи иска может отличаться от текста, предлагавшегося на момент заключения договора, а устаревшая информация, как правило, из сети устраняется). Можно, скажем, принять требование фиксировать производимые в сети действия в какой-либо материальной форме, чтобы потом предъявить зафиксированную таким образом последовательность действий для изучения (неважно, в виде распечатки на бумаге или файла на магнитном диске). Однако не составит труда совершить подделку документа, внести изменения в него "задним числом", особенно для квалифицированного программиста. Помимо чисто текстовой информации в сети циркулирует информация в графической и даже аудиовизуальной форме. Такая информация также может стать предметом изучения при решении спорных юридических вопросов, но уже в качестве не только письменных, но и вещественных доказательств. Даже свидетельские показания по поводу действий, совершаемых пользователями "Интернета", могут основываться не на том, что свидетель лично видел или слышал, а на том, что он получал или рассылал в виде сообщений электронной почты, "начальных страниц" и т.д. Очевидно, подобные вопросы будут иметь тесную связь с уголовно-правовым преследованием нарушений в сфере компьютерной деятельности и способны радикально дополнить и расширить подходы к принятию и изучению доказательств как в уголовном, так и в гражданском процессе.

Заключение

Основные выводы по работе следующие:

1.Ответственность за совершение мошенничества предусмотрена ст.159 УК РФ. Мошенничество - это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Под хищением понимаются совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества.

Мошенничество является формой хищения, поэтому ему присущи все признаки этого понятия. При мошенничестве способом завладения чужим имуществом является обман или злоупотребление доверием. При совершении данного преступления потерпевшая сторона сама передает имущество преступнику, полагая, что последний имеет право на его получение. При этом именно обман или злоупотребление доверием побуждает собственника или иного законного владельца передать преступнику имущество или имущественное право.

Интернет находится в настоящее время в какой-то мере вне законодательного регулирования и контроля государственных органов, что порождает различные правонарушения и преступления под действием нескольких факторов, которые существенно влияют на криминогенную обстановку, сложившуюся вокруг Интернета, одним из которых выступает возможность мошенничества при заключении сделок через Интернет, возможность хищения из виртуальных магазинов, а также создания виртуальных финансовых пирамид.

При мошенничестве Интернет выступает только как средство распространения ложной информации (обмана как обязательного признака мошенничества). Информация в Интернете сама по себе объектом хищения быть не может, так как не является вещью.

Наиболее распространённые виды мошенничества с использованием Интернета связаны с безналичными денежными расчётами и с рынком ценных бумаг. Типичные схемы мошенничества в финансово-кредитной и фондовой сфере приводятся в работе.

3.Анонимность, которую предоставляет своим пользователям сеть Интернет, возможность охвата большой аудитории, высокая скорость и гораздо более низкая стоимость распространения информации по сравнению с традиционными средствами, делает Интернет наиболее удобным инструментом для мошеннических действий. В связи с этим особо актуальной становится проблема борьбы с мошенничеством и иными компьютерными преступлениями, и эта борьба должна осуществляться на двух уровнях – национальном и международном. Правоохранительная деятельность отечественных государственных структур здесь малозаметна. Пользователи сети руководствуются своими писаными и неписаными правилами поведения, но далеко не все они готовы добровольно соблюдать правовые нормы. Преступники же находят все новые и новые возможности применения своих криминальных способностей в Интернете, и они не должны оставаться безнаказанными.

Важно, чтобы правоохранительные органы государства были не просто готовы к нейтрализации обозначенного негативного потенциала сети, но и чтобы они заняли в этом вопросе активную позицию. В частности, хотелось бы, чтобы они проявляли большую активность в сфере профилактики и выявления преступлений, совершаемых посредством сетей Интернет.

Список использованной литературы

I. Нормативно-правовые акты

1. Конституция Российской Федерации. Принята 12 декабря 1993 г.

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. №63-ФЗ.

3. Гражданский кодекс Российской Федерации. Часть первая; от 30 ноября 1994г. №51-ФЗ (с последующими изменениями и дополнениями).

4. Закон Российской Федерации Об авторском праве и смежных правах от 9 июля 1993 г. №5351-1 (в ред. Федерального Закона от 129 июля 1995 г. №11003).

5. Патентный Закон Российской Федерации от 23 сентября 1992 г. (в ред. Федерального Закона от 7 февраля 2003 г.).

6. Постановление Пленума Верховного Суда СССР от 11 июля 1972 г. №4 О судебной практике по делам о хищениях государственного и общественного имущества (с изменениями и дополнениями от 21 сентября 1977 г, 27 ноября 1981 г, 26 апреля 1984 г, а также изменениями, внесенными Пленумом Верховного суда РФ 7 августа 1996 г).

7. Постановление Пленума Верховного Суда СССР от 7 июля 1983 г. №4 О практике применения судами законодательства об охране природы.

8. Постановление Пленума Верховного Суда СССР от 5 сентября 1986 г. №11 О судебной практике по делам о преступлениях против личной собственности.

9. Постановление Пленума Верховного Суда РСФСР от 23 декабря 1980 г. №6 О практике применения судами Российской Федерации законодательства при рассмотрении судами дел на транспорте (с изменениями от 25 апреля 1995 г.).

10. Постановление Пленума Верховного Суда РФ от 25 апреля 1995 г. №5 О некоторых вопросах применения судами ответственности за преступления против собственности.

11.Положение о безналичных расчетах в Российской Федерации. Утверждено Банком России 3 октября 2002 г. №2-П.

12. Положение о порядке осуществления безналичных расчетов физическими лицами в Российской Федерации. Утверждено Банком России 1 апреля 2003 г. №222-П.

II. Литература

13. Гражданское право/под ред. А.П. Сергеева и Ю.К. Толстого. В 3 т.т. - т.1. М.: Проспект, 2003 - 776с.

14. Комментарий к Уголовному кодексу Российской Федерации, /под ред. Ю.И. Скуратова и В.М. Лебедева. М.: Инфра-М, Норма, 1997 -832с.

15. Комментарий к части первой Гражданского кодекса РФ для предпринимателей./сост. М.И. Брагинский. М.: Юристь, 2002-512с.

16. Основы государства и права/под ред. С.А. Комарова. М.: Манускрипт, 1998-320с.

17. Уголовное право Российской Федерации/т. 1. - Общая часть, т.2. - Особенная часть. Под ред. Б.В. Здравомыслова. М.: Юристь, 2003-560 с.

18. Алексеева Д.Г., Пыхтин С.В., Хоменко Е.Г. Банковское право М.: Юристь, 2002 - 480 с.

19. Баяхчев В.Г., Улейчик В.В. Расследование хищений, совершаемых в кредитно-финансовой сфере с использованием электронных средств. // Законодательство. Право для бизнеса. 2000, №6, с.53-59.

20. Безверхое А.Г. Собственность и имущественные отношения в уголовном праве. //Законодательство. Право для бизнеса. 2002, №12, с.50-56.

21. Борзенков Г. Новое в уголовном законодательстве о преступлениях против собственности.// Законность, 1997, №2, с. 7-15.
22. Герцева Е. Н. Проблемы квалификации недобросовестного использования доменных имен в Интернете //Законодательство, N 11, ноябрь 2000 г.
23. Голубев В. В. Интернет и оперативно-розыскная деятельность //Законодательство, 1999, N 11
24. Горелов А.П. Что охраняют уголовно-правовые нормы об ответственности за экономические преступления?.//Законодательство. Право для бизнеса. 2003, №4, с.80-85.
25. Демьянова К. Интернет - средство массовой информации? // Законодательство, N 9, сентябрь 2000 г.
26. Иванов Н.Г. Принцип субъективного вменения и его реализация в УК РФ.// Государство и право, 1999, №10, с.52-58.
27. Калятин В.О Проблемы установления юрисдикции в Интернете //Законодательство, N 5, май 2001 г.
28. Калятин В.О. Гиперссылки в сети интернет как правовая проблема. //Законодательство, N 10, октябрь 2001 г.)
29. Клепицкий И.А. Имущественные преступления: сравнительно-правовой аспект. //Законодательство. Право для бизнеса. 2000, №1, с.61-68; №2, с.72-84.
30. Копылов В.А. Информационное право. М.: Юристь, 2002-512с.
31. Ломидзе О., Ломидзе Э. Крупные сделки хозяйственных обществ: проблемы правового регулирования.// Хозяйство и право, 2003, №1, с.60-74.
32. Наумов А.В. Проблемы совершенствования Уголовного Кодекса Российской Федерации// Государство и право, 1999, №10, с.45-51.
33. Рузакова О. А., Дмитриев С. С. Авторские и смежные права в Интернете //Законодательство, N 9, сентябрь 2001 г.

34. Седугин П.И. Жилищное право. М.: Норма, 2002-384с.
35. Якушев М. А. Интернет и право //Законодательство, 1997, N 1
36. Якушев М. А. Как отрегулировать Интернет? //Законодательство, N 9, сентябрь 2000 г.
37. Яни П.С. Преступное посягательство на имущество. // Законодательство. Право для бизнеса, 1998, №9, с.70-78; №10, с.74-82.