НЕКОТОРЫЕ ОСОБЕННОСТИ МОШЕННИЧЕСТВА, СОВЕРШАЕМОГО В СФЕРЕ И С ИСПОЛЬЗОВАНИЕМ ВЫСОКИХ ТЕХНОЛОГИЙ

Д.О Теплова
аспирант кафедры уголовного права
и криминологии БГУЭП

Статья посвящена рассмотрению необходимости криминализации мошенничества в сфере высоких технологий как квалифицированного вида мошенничества в экономической деятельности и уголовно-правовому анализу состава данного преступления.

The article dwells upon fraud in the sphere of high technologies, makes an analysis of its corpus delicti within the framework of criminal law; it covers the necessity of criminalization and distinguishing fraud in high-tech as aggravated crime in the sphere of economic activity[1].

Согласно ст. 159 Уголовного кодекса РФ под мошенничеством понимается хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Актуальность исследования отдельных аспектов мошенничества определяется, прежде всего, высокой степенью распространенности данного преступления, что напрямую связано с общим экономическим развитием современного общества. Все большее распространение сегодня приобретает мошенничество в сфере высоких технологий. Стремительное развитие указанной сферы, появление новых видов преступлений, совершаемых с помощью системы ЭВМ и их сети требуют всестороннего изучения данной проблемы.

Проблема мошенничества в сфере высоких технологий характеризуется следующими обстоятельствами: повышенной общественной опасностью данного вида деяний и отсутствием законодательно закрепленной уголовно-правовой нормы об ответственности за мошенничества в сфере высоких технологий.

Отдельным проблемам уголовно-правовой охраны собственности от мошеннических посягательств с использованием сферы высоких технологий в отечественной юридической литературе уделялось внимание. Вопросы мошенничества в сфере Интернет рассматривали Л.В. Горшкова, Д.А. Зыков, Л.М. Исаева, Т.П. Кесарева, С.П. Кушниренко, А.Л. Осипенко, А.Е. Шарков и др. Рассмотрением вопросов мошенничества в сетях сотовой связи занимались Н.П. Бирюков, Б.Д. Завидов, Г.В. Семенов, З.А. Ибрагимова, И.В. Лазарева и др. Однако необходим комплексный уголовно-правовой анализ мошенничества этого вида.

Целью данной статьи является выделение мошенничества в сфере высоких технологий как отдельного состава преступления против

[1] Teplova D.O. Some characteristics of fraud committed in the sphere of high-tech and with the use of high technologies.

собственности и квалифицированного вида мошенничества в экономической сфере, а также уголовно-правовой анализ состава данного преступления.

Высокие технологии (англ. high technology, high tech, hi-tech) – это наиболее новые и прогрессивные технологии современности. Сюда входят такие отрасли, как микро- и наноэлектроника, квантовая и оптическая электроника, радиоэлектроника, вычислительная техника, системы хранения данных, интернет-технологии, беспроводные технологии, микро- и нано-электромеханические системы (MEMS/NEMS), технологии энергосбережения и альтернативная энергетика, биометрика, системы контроля и управления доступом, оборонные технологии и технологии двойного назначения, биотехнологии.

Как справедливо отмечает В.А. Мазуров, высокие технологии – это не только компьютеры и сети, но еще и телефоны, специальная техника для негласного получения информации, причем возможности использования в преступных целях высоких технологий постоянно расширяются в связи с внедрением новейших достижений[1].

В качестве примера можно привести фабулу следующего уголовного дела. Между НПО «Сапфир» и германской фирмой был заключен годовой контракт на поставку в ФРГ партии монокристаллических пластин для изготовления солнечных батарей. Зарубежные партнеры перечислили в качестве аванса почти два миллиона евро. Но руководство НПО, получив деньги, продукцию в Германию не отправило и деньги не возвратило. По подозрению в совершении мошенничества в особо крупном размере был арестован генеральный директор ЗАО НПО «Сапфир» К. По мнению следствия, контрагенту причинен ущерб на сумму 63 млн 545 тыс. руб. Было возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 4 ст. 159 УК РФ[2].

Рассматривая указанный вид мошенничества, следует исходить из того, что способ совершения данного преступления (обман или злоупотребление доверием) неразрывно связан со сферой высоких технологий и реализуется в ней посредством этой сферы. Повышенную общественную опасность мошенничеству в сфере высоких технологий придает тот факт, что оно совершается с использованием виртуального пространства (системы ЭВМ и их сети (локальные и глобальные), средств сотовой связи и т.д.).

Официальной статистики по мошенничеству в сфере высоких технологий на данный момент не существует, поскольку в законодательном порядке это преступное деяние отдельно не выделено. Все мошеннические операции в сети сотовой связи квалифицируются либо как мошенничество (ст. 159 УК РФ), либо как причинение имущественного ущерба путем обмана или злоупотребления доверием при отсутствии признаков хищения (ст. 165 УК РФ). Этот процесс, по мнению Б.Д. Завидова и З.А. Ибрагимовой, не отражает латентности указанного преступного деяния, которая намного выше, чем у простого мошенничества[3].

Уголовный кодекс РФ сферу высоких технологий ограничивает только посягательствами на общественные отношения в сфере компьютерной информации, что отражено в главе 28 УК РФ. Так, С.С. Медведев отмечает, что состав мошенничества позволяет квалифицировать хищения путем

обмана и злоупотребления доверием в сети Интернет только по части первой (преступление небольшой тяжести). Использование сети Интернет в мошеннических действиях, значительно повышающее их общественную опасность, законодателем не учитывается[4]. Этот подход не позволяет охватить уголовным законом основную массу опасных посягательств в сфере высоких технологий. При этом следует подчеркнуть, что ст. ст. 159 и 165 УК РФ не способны отразить все варианты и повышенную общественную опасность использования высоких технологий в мошенничестве.

Глава 28 УК РФ «Преступления в сфере компьютерной информации» содержит в себе три статьи. Диспозиция ст. 272 УК РФ допускает уголовную ответственность только за факт и неправомерность доступа к компьютерной информации. Статья 273 УК РФ предусматривает уголовную ответственность лишь за создание, использование и распространение вредоносных программ для ЭВМ. Следует отметить, что ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» применима лишь к лицу, которое в силу своих служебных полномочий (функций) имело доступ к ЭВМ, системе ЭВМ или их сети.

Таким образом, действия по хищению денежных средств с помощью проникновения в систему сети Интернет, в базу данных ЭВМ не охватываются рамками главы 28 УК РФ.

Рассмотрим способы мошенничества в сфере высоких технологий.

Способы совершения мошенничества в сетях сотовой связи классифицируются авторами по-разному. В результате изучения научной литературы и анализа имеющихся точек зрения можно предложить следующую классификацию:

- подписной фрод (subscription fraud) – злостные неплатежи при интенсивном пользовании сотовой связью[5];

- технический фрод – использование в дублирующем и основном абонентском аппарате одних и тех же идентификаторов, при этом плата за вызовы с дублирующего аппарата включается в счет владельца основного аппарата[6];

- кража и подделка телефонных карточек, обеспечивающих безвозмездное получение услуг телефонной связи;

- неправомерное получение кодов доступа к телефонным линиям с целью бесплатного получения услуг телефонной связи;

- перекодирование сотовых телефонов для бесплатного получения услуг связи;

- неправомерное получение серийных и идентификационных номеров сотовых телефонов для невозможности их идентификации и бесплатного получения услуг связи[7].

Четыре вида мошенничества в сетях сотовой связи выделяет Г. Семенов:

- контрактное мошенничество – использование абонентами услуг связи без оплаты (мошенничество с использованием заключенного контракта и мошенничество при использовании услуг льготного тарифа);

- хакерское мошенничество – проникновение в незащищенную систему и использование либо последующая продажа имеющихся в системе

функциональных возможностей (использование в целях мошенничества УАТС (местной АТС) и хакерское нападение на сеть);

- внутрикорпоративное техническое мошенничество – внесение изменений сотрудниками компаний в определенную внутреннюю информацию с целью получения доступа к услугам по сниженной стоимости;

- процедурное мошенничество включает атаки на процедурные алгоритмы, предназначенные для уменьшения риска мошенничества (неправомочное использование режимов роуминга, дублирование идентификаторов телефонных карт (смарт-карт), использование фальшивых телефонных карт)[8].

В качестве примера мошенничества в сетях сотовой связи можно привести следующее уголовное дело. К. приобрел сотовый телефонный аппарат, который обладал возможностью использовать при производстве телефонных звонков абонентские номера легальных владельцев сотовых телефонных аппаратов сотовой сети «ВОТЕК МОБАЙЛ». Впоследствии гр. К. наряду с другими лицами неоднократно сканировал (перехватывал) идентификационные номера легальных пользователей и вносил их в память аппарата, а затем производил телефонные звонки за счет легальных абонентов «ВОТЕК МОБАЙЛ»[9].

Одну из типовых схем мошенничества в сетях сотовой связи использовал гр. С. Он заключил контракт на обслуживание в роуминге с оператором ОАО «Мегафон». Затем приобрел кредитную карту у другого оператора. Став роумером, в новой сети он совершил звонки в Норвегию, Испанию и Египет общей продолжительностью более 200 минут, заранее замышляя их не оплачивать. Звонки С. делал до тех пор, пока ему не было отказано в доступе[10].

Необходимо также рассмотреть, каким образом совершается мошенничество в системе Интернет и сетях ЭВМ. А.В. Корягин выделяет следующие способы, которые имеют массовое распространение:

- приобретение противозаконными средствами или открытие, перемещение или использование торговой, коммерческой, промышленной тайны без соответствующего разрешения или иных законных оснований с целью нанесения экономического вреда лицом, который имеет доступ к тайне, или получение противозаконного экономического преимущества для себя или других лиц;

- нарушения с идентификаторами доступа (логин-пароли, PIN-коды);

- посягательства на информацию с ограниченным доступом с использованием технологий удаленного доступа, в том числе несанкционированный перехват информации с помощью технических средств связи как в рамках компьютера, системы или сети, так и вовне ее[11].

Следующим способом мошенничества в сфере высоких технологий является совершение преступлений с компьютерными учетами, доступ к которым обеспечивается удаленно через сетевые технологии. В частности, довольно распространено незаконное использование преступниками систем «Клиент–Банк» в отношении либо предприятий (учреждений), либо для обеспечения эффективного управления электронными денежными активами преступной деятельности.

Для иллюстрации данного способа мошенничества можно привести следующий пример. Управляющий ГОУП «Балтинвесттранс» К. путем злоупотребления доверием со стороны директора ГОУП и обмана бухгалтера предприятия И. узнал учетный код и пароль предприятия в системе «Клиент–Банк» и, воспользовавшись этими данными, перевел со счета предприятия 500 тыс. руб. на заранее открытый на подставное лицо расчетный счет в коммерческом банке как оплату за поставленный товар. В тот же день счет, на который были переведены деньги, был закрыт. Черемухинским районным судом г. Москвы действия К. были квалифицированы по совокупности по ст.ст. 272 и 159 УК РФ[12].

Наиболее распространены кражи со счетов различных платежных систем WEBMONEY, «Яндекс деньги» и так далее, причем в данном случае схема мошенничества может быть чрезвычайно простой.

Так, из материалов дела, рассмотренного Чертановским районным судом г. Москвы, следует, что ООО «Троя» заключило договор поставки продукции, выбранной в Интернет-магазине. Договор был заключен путем обмена сторонами файлов, содержащих текст договора и скреплен электронной цифровой подписью. После чего в адрес ООО «Троя» по E-mail поступило письмо с подтверждением отгрузки интересующего товара и предложением перевести предварительную плату за товар с использованием электронной системы платежных переводов WEBMONEY. После оплаты товара поставки продукции не произошло. Во время переговоров с ООО «Троя» гражданин М. (якобы действующий от лица Интернет-магазина, представившись его представителем) пояснил, что товар был задержан на таможне и для его выкупа необходимо внести штраф в размере 200 тыс. руб. Штраф также предлагалось перечислить с использованием электронной системы платежных переводов WEBMONEY. В результате мошеннических действий М. ООО «Троя» был нанесен значительный ущерб. Действия М. были квалифицированы судом по ст. 159 УК РФ[13].

В процессе исследования судебной практики было выявлено, что самым массовым способом мошенничества в сфере высоких технологий являются нарушения с идентификаторами доступа в целях посягательства на информацию с ограниченным доступом, незаконное использование систем управления электронными денежными активами и кражи со счетов различных электронных платежных систем.

Анализируя такой частный вид мошенничества, как мошенничество в сфере высоких технологий, необходимо дать следующую характеристику. Что касается родового объекта, то следует согласиться с мнением ученых, полагающих, что «родовой объект – это группа общественных отношений и интересов, взятых под охрану специально предусмотренным комплексом норм Особенной части УК РФ»[14].

Определяя родовой объект посягательства при мошенничестве, представляется целесообразным принять мнение исследователей в данной области, которое сводится к тому, что «родовым объектом преступлений против собственности, как и других преступлений в сфере экономики, являются общественные отношения и интересы в сфере производства,

обмена и распределения продукции и услуг в широком смысле слова»[15]. Исходя из этого, родовым объектом мошенничества, вероятное всего, выступает совокупность образующих частногражданскую сферу экономических отношений, охраняемых уголовным законом в целях предотвращения возможности возникновения общественной опасности, выражающейся в подрыве гарантированного государством права частной, государственной, муниципальной, общественной и иной формы собственности. Непосредственным объектом при мошенничестве являются права владения, пользования и распоряжения собственностью.

Объективная сторона мошенничества в сфере высоких технологий выражается в действиях – хищении чужого имущества и приобретении права на чужое имущество с использованием ЭВМ, локальных и глобальных компьютерных сетей, электронно-технических устройств, предназначенных для создания, хранения, передачи, изменения, копирования, удаления и иных действий с информацией в электронном виде и способе такого хищения и приобретения – обмане или злоупотреблении доверием.

Обман при совершении компьютерных мошенничеств состоит в сознательно неправильном оформлении компьютерных программ, несанкционированном воздействии на информационный процесс, неправомерном использовании банка данных, применении неполных или дефектных, искаженных программ с целью получения чужого имущества или права на него.

Авторы комментария к Уголовному кодексу РФ под редакцией А.В. Наумова указывают, что исходным моментом при рассмотрении хищения является его предмет, т.е. имущество. В отличие от объекта, которым является отношение собственности, предмет хищения всегда материален, так как служит частью материального мира. В частности, не могут быть предметом хищения достижения человеческого разума (идеи, взгляды), лишенные признака вещи[16].

Данная трактовка понятия «предмет хищения» в условиях современного развития социально-экономических отношений, НТР и стремительного развития компьютерных и иных технологий, все большего использования виртуальных платежных систем представляется слишком узкой и способствует уходу причинителя вреда от уголовной ответственности. В этой связи представляется целесообразным согласиться с мнением авторов, считающих, что предмет хищения (как и предмет преступления в целом) может выступать не только в материальной, но и в виртуальной форме[17].

Обращаясь к субъекту мошенничества в сфере высоких технологий, следует отметить, что им будет являться вменяемое физическое лицо, достигшее возраста 16 лет. Думается, что это не соответствует объективной действительности, в которой процесс формирования личности, в том числе и преступной, многократно превысил нижний предел, установленный законодателем ранее. Напрашивается вывод о том, что необходимо снизить возраст наступления уголовной ответственности за мошенничество до 14 лет. Такое предложение связано с тем, что информационные технологии

развиваются интенсивно, и возраст лиц, совершающих преступления в данной сфере, стремительно «молодеет».

Кроме того, следует отметить, что в совершение мошенничества в сфере высоких технологий вовлекаются лица, профессионально занимающиеся программированием и компьютерными сетями. Поэтому следует выделить специальный субъект мошенничества в сфере высоких технологий – лиц, профессионально занимающихся программированием и компьютерными сетями.

Субъективная сторона мошенничества в сфере высоких технологий аналогична «традиционному» мошенничеству, т.е. характеризуется прямым умыслом и корыстной целью.

Дополнительным признаком мошенничества в сфере высоких технологий является факт осознания лицом, совершающим общественно опасное деяние, своей отдаленности от жертвы. При общении через сеть Интернет, средства сотовой связи жертва не видит злоумышленника. Особенно это влияет на решимость совершить преступление, когда субъект преступления и жертва разделены границами не только государств, но и континентов. Кроме того, субъект мошенничества в сфере высоких технологий обладает специальными знаниями и навыками, это обусловливает его постпреступное поведение.

Несмотря на виртуальность предмета мошенничества, состав мошенничества в сфере высоких технологий материальный. В материальном составе диспозиция предусматривает конкретное преступное последствие. Данное преступное последствие выражается в причинении материального вреда.

На основании изложенного необходимо констатировать факт повышенной общественной опасности мошенничества в сфере высоких технологий по сравнению с простым мошенничеством. В связи с этим законодателю необходимо принять меры по его криминализации.

Предлагается дополнить ст. 159 УК РФ «Мошенничество» ч. 5 в следующей редакции:

«Мошенничество с использованием ЭВМ, локальных и глобальных компьютерных сетей, электронно-технических устройств, предназначенных для создания, хранения, передачи, изменения, копирования, удаления и иных действий с информацией в электронном виде, – наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо лишением свободы на срок от трех до пяти лет».

Есть вероятность того, что предлагаемая редакция позволит криминализировать мошеннические деяния в сфере высоких технологий и судам назначать адекватное наказание виновным лицам. Представляется, что в дальнейшем при более глубокой проработке вопросов преступности в сфере высоких технологий, станет возможным ввести в Уголовный кодекс РФ отдельную статью «Мошенничество с использованием высоких технологий», предусмотрев простой и квалифицированный состав данного преступления.

В заключение можно сделать следующие основные выводы:

1. Необходимо констатировать факт повышенной общественной опасности мошенничества в сфере высоких технологий по сравнению с простым мошенничеством. На сегодняшний день уровень криминализации общественно опасных деяний в сфере высоких технологий не отвечает реальному положению вещей. Причиной данного явления может быть недостаточное изучение проблем компьютерной преступности и стремительное развитие самой сферы высоких технологий.

2. Целесообразно выделение мошенничества в сфере высоких технологий как отдельного состава преступления против собственности и особо квалифицированного вида мошенничества. Факт необходимости введения такой нормы у законодателя не должен вызывать никаких сомнений, так как недооценка борьбы с вышеуказанными действиями, носящими, безусловно, противоправный характер, может привести к самым негативным последствиям.

3. В дальнейшем необходимо продолжить научные исследования проблем криминализации общественно опасных деяний в сфере высоких технологий для создания и совершенствования теоретической базы противодействия компьютерной преступности.

ПРИМЕЧАНИЯ

[1] См.: Мазуров А.В. Преступность в сфере высоких технологий: понятие, общая характеристика, тенденции / А.В. Мазуров // Вестник Томск. гос. ун-та. 2007. № 2. С. 151 – 154.

[2] См.: Федосенко В. Цена высоких технологий. Гендиректор подозревается в присвоении двух миллионов евро / В. Федосенко // Рос. газ. 2008. 22 апр.

[3] Завидов Б.Д. Мошенничество в сфере высоких технологий / Б.Д. Завидов, З.А. Ибрагимова // Современное право. 2001. № 4. С. 43.

[4] Медведев С.С. Мошенничество в сфере высоких технологий: автореф. … канд. юрид. наук / С.С. Медведев. Краснодар, 2008. С. 17-18.

[5] См.: Ратынский М.В. Телефон в кармане / М.В. Ратынский, А.В. Телегин. М.: Радио и связь, 2000. С. 174-175.

[6] Там же.

[7] См.: Крылов В.В. Расследование преступлений в сфере компьютерной информации / В.В. Крылов. М.: Городец, 1998. С. 197-198.

[8] Семенов Г. Криминалистическая классификация способов совершения мошенничества в системе сотовой связи / Г. Семенов // Информост – радиоэлектроника и телекоммуникации. 2001. № 3(16). С. 30.

[9] Постановление Чертановского районного суда г. Москвы от 22.02.2008 г. // Архив Чертановского районного суда г. Москвы.

[10] Там же.

[11] Корягин А.В. Преступность в сфере компьютерных и интернет-технологий: актуальность и проблемы борьбы с ней / А.В. Корягин. Режим доступа: http://www.crime-research.ru/library/Koragin.html. – Дата доступа: 16.03.2009.

[12] Определение Черемухинского районного суда г. Москвы от 28.03.2007 г. // Архив Черемухинского районного суда г. Москвы.

[13] Постановление Чертановского районного суда г. Москвы от 12.05.2007 г. // Архив Чертановского районного суда г. Москвы.

[14] Уголовное право России. Практический курс: учебно-практ. пособие/ под общ. ред. А.И. Бастрыкина М.: Волтерс Клувер, 2007. С. 59.

[15]Там же.

[16]Комментарий к Уголовному кодексу РФ / под ред. А.В. Наумова. М.: Норма, 2006. С. 396-397.

[17]См.: Шульга А.В. Объект и предмет преступлений против собственности в условиях рыночных отношений и информационного общества / А.В. Шульга. Дата доступа: 14.03.2009. Режим доступа: http://vak.ed.gov.ru/common/img/uploaded/files/vak/announcements/yuridicheskie/14-04-2008/SHulgaAV.doc