Преступления в банковской сфере 17-21 июля 2004

Налетчиков едва не застрелили из их пистолета
17.07.2004, Москва
Московский комсомолец

Дерзкое вооруженное ограбление инкассаторов, перевозивших заработную плату для рабочих-железнодорожников, предприняли в четверг четверо преступников на проспекте Мира. Разбойники завладели зарплатой рабочих на сумму 4,5 миллиона рублей, но потеряли во время бегства с места происшествия свой пистолет и едва не угодили под свои же пули!
Как стало известно "МК", главный бухгалтер Московского отделения Рижского направления МЖД вместе с прорабом и водителем предприятия отправились за деньгами в банк. За заработной платой для рабочих "Газель" ездит каждый месяц в определенный день по одному и тому же маршруту, поэтому преступникам не составило труда вычислить место и время для нападения. Упаковав купюры в большую сумку, сотрудники предприятия отправились обратно, но возле дома 79 по проспекту Мира грузовичок неожиданно "подрезали" "Жигули" 9-й модели. Водитель "Газели" был вынужден ударить по тормозам, а из "девятки" выскочили трое молодых людей. Стекло со стороны водителя было поднято, однако это не остановило налетчиков. Один из них рукояткой пистолета "ТТ" разбил стекло. Другой грабитель брызнул из газового баллончика в глаза даме-бухгалтеру и выхватил у нее из рук сумку с деньгами.
Бандиты вместе с добычей бросились наутек, однако в суматохе один из нападавших обронил пистолет. Этим обстоятельством воспользовался 50-летний прораб-железнодорожник и, подобрав оружие, выстрелил по машине грабителей. Впрочем, пуля просвистела мимо, и мужчина не стал далее рисковать и палить из оружия на оживленной улице.
Брошенную неподалеку машину преступников позже обнаружили милиционеры. Выяснилось, что на "девятке" стоят краденые номера. Более того, сама машина оказалась угнанной, да еще и с перебитыми номерами на кузове и двигателе. Сейчас милиция занимается поисками бандитов, и не исключено, что к ограблению может быть причастен кто-то из работников железной дороги

Зерновая "пирамида" для банкиров
17.07.2004
Русский курьер

Еще и десяти лет не прошло с тех пор, как на просторах России орудовали печальной памяти финансовые компании МММ, "Русский дом Селенга" и прочие "Хопер-инвесты". Казалось бы, потерявший многие свои сбережения в этих "пирамидах" народ на долгие годы вперед получил иммунитет к такого рода мошенничеству. АН нет! Оказалось, что ловушка может работать и до сих пор. И самое удивительное, что попадаются в нее даже не простые обыватели-вкладчики, а умудренные специалисты всеми уважаемых банков. Таких, как Сбербанк, Внешторгбанк, МДМ и многих прочих.
В 2003 году новые строители "пирамид" из холдинга "Русагрокапитал" банально кинули финансистов на десятки миллионов долларов. История "зернового

мошенничества", а также нынешние мучения оказавшихся в нее втянутыми банкиров достаточно проста и поучительна.
ОАО "Русагрокапитал" было создано в 1999 году, и владельцем 99, 9% ее акций являлся кипрский офшор Agro Holdings Ltd. Впрочем, это номинально, реальным же владельцем был русский господин Яков Шляпочник и группа его доверенных товарищей. Предполагалось вести бизнес, создавая агрохолдинг, в который должны были войти предприятия сельхозпереработки из целого ряда регионов страны. Во всяком случае, именно так звучала официальная цель, и для ее реализации начали действительно скупаться элеваторы и заводы в Новосибирской, Свердловской, Тверской, Смоленской, Ростовской и некоторых других областях. Итого за короткий промежуток времени накопилось 8 мукомольных заводов, 3 элеватора и птицефабрика. На какие деньги совершались эти покупки - один из вопросов, на которые предстоит ответить начавшемуся следствию. Но это сейчас, а тогда параллельно с приобретением промышленных активов холдинг начал формировать и собственную кредитную историю, беря небольшие кредиты в банках якобы на развитие производства и закупку сырья. Заметим, что "кредитная история" - вещь для бизнесменов крайне важная. Это своего рода тоже актив, потому что, только зарекомендовав себя прилежным плательщиком, можно рассчитывать на деловые отношения с серьезными банками, то есть опять-таки на получение кредитов, но. уже гораздо больших по объемам.
К началу 2003 года "Русагрокапитал" контролировал около 10% мукомольного рынка страны и 25% рынка масложировой продукции.
Именно в этот момент руководство "Русагрокапитала" и решилось наконец-то сыграть по-крупному. За короткий период в крупнейших банках страны берутся кредиты на общую сумму более 3, 5 миллиарда рублей. Сейчас финансисты сами удивляются, как легко дали себя одурачить. Чуть позже выяснилось, что общая стоимость всех промышленных активов холдинга не превышает 30 миллионов долларов, хуже того, подавляющее большинство предприятий - фактические банкроты, и реализовать их не удастся даже за эту сумму. Но кредиты ведь выдавались под залог имевшегося зерна! И именно здесь была допущена ключевая промашка.
"Русагрокапитал" для разных банков закладывал одно и то же зерно. При этом совсем не в таких объемах, как демонстрировал заимодавцам. В ход шли зернохранилища с двойным дном и прочие уловки, демонстрировавшие гораздо большее количество зерна, чем имелось в распоряжении на самом деле. Когда пришла пора возвращать долги, владельцы холдинга попросту вывезли заложенное-перезаложенное зерно в неизвестном направлении, прихватив при этом еще и зерно, хранившееся на элеваторах холдинга другими компаниями. В этот момент всем участвовавшим в этой истории банкирам стало окончательно понятно, что их кинули. "Кинули" во всем, в том числе и с кредитной историей. Даже попытки самостоятельного расследования показали, что "Русагрокапитал", если и развивался когда-то, то исключительно на свои, неизвестного происхождения деньги. А все шедшие по нарастающей банковские кредиты использовались для погашения предыдущих заимствований - банальная "пирамида". В феврале нынешнего года сменившееся руководство холдинга объявило о собственной несостоятельности и даже с ехидцей заметило, что истребование долгов банками будет чрезвычайно осложнено проблемой "перекрестных залогов".

Проблемы квалификации хищения денежных средств со счетов банка с использованием средств компьютерной техники.
журнал "Российский судья"
июнь 2004

Столкнувшись до введения в действие Уголовного кодекса Российской Федерации с компьютерными преступлениями, правоохранительные органы начали борьбу с ними при помощи традиционных норм о краже, присвоении, мошенничестве, злоупотреблении доверием и других. Однако такой подход оказался не вполне удачным, поскольку многие компьютерные преступления не охватывались составами традиционных преступлений. Это повлекло включение в новый УК РФ главы 28 "Преступления в сфере компьютерной информации". Но и после внесения данной главы в УК РФ на практике возникают проблемы при квалификации того или иного состава преступления по той или иной статье Уголовного кодекса Российской Федерации, связанного со средствами компьютерной техники.

С зарубежным законодательством по-другому: составы компьютерных преступлений (где предметом преступления является охраняемая законом компьютерная информация) либо просто отсутствуют, либо существуют наряду с традиционными составами (мошенничество, выдача государственной тайны, собирание и распространение персональных данных). Последние либо предусматривают самостоятельный состав, который выступает как специальный по отношению к общему (тому же мошенничеству), либо находятся в той же статье в качестве квалифицированного состава.

На наш взгляд, законодатель должен выбрать комплексный подход к охране компьютерной информации и обеспечить наличие в Уголовном кодексе РФ не только самостоятельных составов по компьютерным преступлениям, но и составов, которые бы выступали в качестве специальных по отношению к общим (например, "кража денежных средств со счетов в банках с использованием средств компьютерной техники" - специальный состав, "кража" - общий состав) либо же находились бы в той же статье в качестве квалифицирующего признака (например, ст. 158 ч. 2 п. "д" - "с незаконным проникновением в банковскую или иную компьютерную системы, сеть, ЭВМ, с использованием средств компьютерной техники").

В этом отношении применение соответствующих положений УК РФ 1996 г. является более сложным. Практика применения существующих составов (ст. 272 - 274 УК РФ) невелика, что вызывает немало затруднений и противоречивых квалификаций.

Уголовный кодекс РФ помимо описанных выше составов (ст. 272 - 274), предметом которых является компьютерная информация, не содержит в других главах специальных или квалифицированных составов, связанных с использованием средств компьютерной техники и иных высоких технологий. Предмет преступления, предусмотренного ст. 272 УК, - охраняемая законом компьютерная информация. Однако невозможно представить себе покушение на информацию саму по себе. Если эта информация охраняется законом, то она является либо государственной, либо коммерческой, либо личной тайной и т. п. Следовательно, речь может идти о преступлениях против государственной власти либо преступлениях против конституционных прав и свобод человека и гражданина. Единственное исключение в этом плане составляет оценка действий, направленных на отношения, охраняющие коммерческую и, в ряде случаев, служебную тайну. В связи с этим возникает вопрос: если совершается покушение на охраняемую законом информацию, охватываемое иными статьями УК, достаточно ли будет квалификации по статьям гл. 28 Кодекса либо необходима квалификация по совокупности?

Основными действиями, предусмотренными ст. 272 УК, являются незаконное копирование и распространение программных продуктов для ЭВМ, и хищение денежных средств из разного рода финансовых институтов с помощью обхода компьютерных систем безопасности и подбора паролей. Относительно первой разновидности действий возникает конкуренция норм, предусмотренных ст. ст. 272 и 146 УК РФ. Программы для ЭВМ являются объектами авторских прав. Однако в

литературе зачастую даже не упоминается о нормах главы 28 УК РФ\1. Автор последовательно\2 пишет о признании нарушения только авторского права и соответствующей квалификации по ст. 146 УК РФ (нарушение авторских и смежных прав), а в некоторых случаях и по совокупности со ст. 180 (незаконное использование товарного знака). При компьютерном мошенничестве в юридической литературе имеется точка зрения о необходимости квалификации только по ст. 159 УК РФ либо, в зависимости от обстоятельств дела, по ст. 1 58 УК РФ. Приоритет отдается преступлениям против собственности, в которых средства компьютерной техники являются лишь орудием, средством. По этому же пути идет и судебная практика, которая, правда, весьма скудна. Так, один из московских межмуниципальных судов рассмотрел уголовное дело по факту хищения средств с использованием компьютерной сети Интернет. Гражданин России Г., используя домашний компьютер, в одном из сайтов Интернета обнаружил программу, производящую безналичные расчеты с кредитных карт. Г. скопировал программу на свой компьютер. После этого Г., входя в виртуальный магазин, реальный аналог которого располагался в Канаде, производил заказ и предварительную оплату товаров с чужих кредитных карточек, используя вышеупомянутую программу. После этой трансакции Г. незамедлительно отказывался от приобретения товара, однако для возврата денег указывал уже иные номера кредитных карт - собственных или своих сообщников. При этом последние были как гражданами России, так и Литвы. Деньги либо немедленно обналичивались через банкоматы, либо с помощью кредитных карт производилась покупка товаров в тех магазинах Москвы и Вильнюса, где расчеты возможны также с помощью кредитных карт. На первый взгляд, в данном деянии затронуты три страны. Однако на самом деле их значительно больше, так как пострадавшие лица, с банковских карточек которых незаконно списывались денежные средства якобы в оплату товаров, являлись гражданами различных стран. Гражданин Г. признан судом виновным в совершении преступления, предусмотренного ч. 3 ст. 159 УК РФ\3. Почему не встал вопрос о квалификации преступления по совокупности статей (со ст. 272 УК ФР) не ясно.

Наиболее известным преступлением подобного рода является содеянное российским программистом Владимиром Левиным в группе с рядом других граждан Российской Федерации и зарубежных стран, которые, вступив в сговор с целью хищения денежных средств в крупных размерах, осуществили несколько десятков несанкционированных переводов денег со счетов крупных иностранных банков и корпораций - клиентов крупнейшего в мире City Bank of America\4. Образовав устойчивую преступную группу, они в период с июня по сентябрь 1994 г., используя глобальную компьютерную сеть Internet и преодолев при этом несколько рубежей многоконтурной защиты локальной банковской сети от несанкционированного доступа, с помощью персонального компьютера стандартной конфигурации из офиса АОЗТ "Сатурн", находящегося в Санкт-Петербурге, вводили в систему управления наличными фондами указанного банка ложные сведения. В результате ими было осуществлено не менее 40 переводов денежных средств на общую сумму 10 миллионов 700 тысяч 952 доллара США со счетов клиентов названного банка на счета лиц, входящих в состав преступной группы, проживающих в шести странах: США, Великобритании, Израиле, Швейцарии, ФРГ и России. Большинство специалистов по банковским компьютерным системам считают, что Левин, скорее всего, подставная фигура в грандиозной международной афере. Следствие по делу Левина, начатое в 1994 г., вскрыло преступную группу (в одном только Петербурге в ее состав входило около 20 человек и еще несколько человек в Англии, США и Израиле). О подлинно международном характере этого преступления свидетельствует география его совершения, охватывавшая страны, откуда изымались крупные суммы денег со счетов

клиентов (Аргентина, Гонконг, Индонезия, Канада, Колумбия, Мексика, Новая Зеландия, Уругвай) и страны, куда деньги переводились и где похищались (Россия, Нидерланды, Швейцария, Израиль)\5.
Этот пример подчеркивает, насколько большим может быть ущерб от такого преступления, сложность его раскрытия, судебного разбирательства и привлечения к ответственности.
Эффективность борьбы с преступлениями в банковских информационно-вычислительных системах в значительной мере определяется пониманием криминалистической сущности данного вида преступного посягательства. Рассмотрим такой пример. Некий злоумышленник проник в компьютерную систему банка и, проведя ряд операций, преодолев определенную защиту, перевел некоторую сумму на свой счет.
Это преступление, прежде всего, можно квалифицировать по ст. 272 УК РФ "Неправомерный доступ к компьютерной информации".
В данном случае, как видим, произошло несанкционированное изменение охраняемой законом компьютерной информации, содержащей сведения о счетах клиентов банка (кредитная организация, Банк России гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов\6), то есть модификация информации, что и входит в диспозицию данной статьи. Под неправомерным доступом к компьютерной информации понимается получение с использованием средств компьютерной техники без соответствующего разрешения возможности просматривать эту информацию и (или), совершать с ней какие-либо манипуляции.
Злоумышленник не имел законного права обращаться с такой информацией, поэтому очевидно - произошел неправомерный доступ к компьютерной информации, который вдобавок ко всему еще и сопровождался нейтрализацией средств ее защиты, что уже само по себе может рассматриваться как состав оконченного преступления, подпадающего под действие ст. 272 УК РФ, поскольку такая нейтрализация всегда связана с уничтожением, блокированием, модификацией либо копированием информации, что нарушает правильную работу ЭВМ.
Но в результате действий злоумышленника с чьего-то счета исчезли деньги. То есть произошло хищение - совершенное с корыстной целью противоправное безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или иному владельцу этого имущества (примечание 1 к ст. 158 УК РФ). Это не вызывает сомнения, поскольку присутствуют все объективные признаки хищения:
изъятие и обращение чужого имущества в пользу виновного или других лиц;
причинение этими действиями реального материального ущерба собственнику или иному владельцу этого имущества;
противоправность совершения этих действий;
безвозмездность их совершения;
корыстная цель.
Однако проблема состоит в том, как квалифицировать это хищение. Хищение может быть совершено путем кражи, мошенничества, присвоения или растраты, грабежа или разбоя. В данном случае, естественно, речь не может идти ни о растрате, ни о присвоении чужого имущества, и уж конечно ни о грабеже или разбое.
Необходимым признаком кражи является тайное хищение чужого имущества. И это, с одной стороны, присутствует в рассматриваемом случае. Но собственно деньги, как материальный предмет, украдены не были - были только изменены определенные реквизиты в электронных записях, что привело к изменению прав на владение и распоряжение имуществом (деньгами). То есть отсутствует предмет кражи - материальное имущество так как "деньги" существуют тут не в виде вещей, а в виде

информации на компьютерном носителе. Собственно компьютерная информация не может быть предметом преступлений против собственности, определенных Уголовным Кодексом Российской Федерации, потому что она не отвечает одному из основных признаков предмета таких преступлений, - она не обладает физическим признаком.
Речь о краже может идти лишь тогда, когда преступник после перевода на свой счет денег пришел в банк и снял их со счета, то есть завладел ими и получил возможность распоряжаться по своему усмотрению, реально стал ими распоряжаться. Такое реальное распоряжение также возможно, если преступник их не получил "на руки", а пустил их в оборот под проценты или иной оборот для получения большей выгоды в том же электронном виде. В этом случае получается, что преступник уже стал реально распоряжаться деньгами, которые еще и не обрели материальную основу.
Хочу заметить, что ряд авторов (например: Э.С. Тенчов, С. В. Вихорев, В. Г. Герасименко) считают, что в данном случае присутствует обман, в результате которого и были переведены чужие деньги. А значит, данное деяние можно квалифицировать по ст. 159 УК РФ - мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана. Под обманом понимается умышленное искажение или сокрытие истины с целью введения в заблуждение лица, в ведении которого находится имущество, приводящее к добровольной его передаче преступнику. Кроме того, обман предполагает, что сам потерпевший, собственник или владелец вещи вследствие такового обмана выводит имущество из своего владения, то есть добровольно передает его преступнику, представляет последнему в отношении имущества правомочия владения, пользования и даже распоряжения, если имущество передается в собственность. Вряд ли в рассматриваемом случае можно усмотреть "добровольность" передачи денег. Трудно согласиться и с наличием в этой ситуации обмана. Обман кого имеет место - именно кого, а не чего? Обман предполагает введение в заблуждение собственника (владельца) имущества, а в нашем случае имеется "обман" компьютерной системы. О таком "обмане" возможно лишь говорить при создании искусственного интеллекта. Хотя, все зависит от способа проникновения в информационную банковскую систему. Например, возможен обман оператора банка при аутентификации пользователя с удаленной ЭВМ (пароль, цифровая подпись и т.п.) Но и в таком случае обман не будет характерен для мошенничества, поскольку он используется не для завладения чужим имуществом, а для облегчения хищения путем получения доступа к банковской системе. Оценивать содеянное только как преступление против собственности нет достаточных оснований и потому, что информация сама по себе не может служить предметом преступлений против собственности ввиду несоответствия обязательным признакам предмета. Поэтому, на наш взгляд, данное преступление как мошенничество квалифицировать нельзя.
Посмотрим все-таки, в какой момент преступления совершается таковой обман. Память компьютера можно рассматривать как место, где в электронном виде хранится информация о денежных средствах, позволяющая проводить операции с ними. При этом, как правило, используются специальные программно-аппаратные средства защиты от несанкционированного доступа к этой информации.
Преступник может использовать обман только в момент проникновения в компьютерную сеть банка, при преодолении системы ее защиты, причем только при конкретном методе, то есть с обманом живого человека, а не ЭВМ.
Но тогда в соответствии с ч.2 ст. 158 п. "б" это действие, по нашему мнению, можно рассматривать как "незаконное проникновение в помещение, либо иное хранилище". Ведь проникновением признается и вторжение в хранилище с помощью приспособлений (в нашем случае с помощью компьютера), а также путем использования обмана. Проникновение не является самоцелью преступления, а

является только способом получения доступа к хранящимся ценностям. Под иным хранилищем понимается особое устройство или место в ЭВМ, системе ЭВМ или их сети, "иные сооружения, которые оборудованы техническими средствами или обеспечены иной охраной и предназначены для постоянного или временного хранения материальных ценностей"\7 .

Рассматриваемый нами случай, таким образом, может быть квалифицирован как кража, совершенная с проникновением в иное хранилище (ч.2 ст.158 п. "б").

Необходимо также отметить, что хищение признается оконченным преступлением только с момента фактического изъятия имущества и наличия у злоумышленника реальной возможности распоряжаться им по своему усмотрению. В данном случае такая возможность появляется с момента завершения трансакции и реализуется путем снятия денег или запуском их в коммерческий оборот.

В целом, хищение денежных средств со счетов банка с использованием средств компьютерной техники целесообразно квалифицировать по ст. 158 ч. 2 п. "б" УК РФ и по соответствующей части ст. 272 УК РФ.