Abzalova Xurshida Mirziyatovna
Yuridik fanlar doktori, dotsent Toshkent davlat yuridik universiteti

ONLAYN-BANKING SOHASIDAGI FIRIBGARLIKNI KVALIFIKATSIYA QILISH

Abzalova Khurshida Mirziyatovna
Doctor of Law, Associate Professor Tashkent State law university

ONLINE BANKING FRAUD QUALIFICATION

Абзалова Хуршида Мирзиятовна
Доктор юридических наук, доцент Ташкентский государственный юридический университет

КВАЛИФИКАЦИЯ МОШЕННИЧЕСТВА В СФЕРЕ ОНЛАЙН-БАНКИНГА

В настоящее время в сфере банковской деятельности активно применяются так называемые «высокие технологии», в том числе системы дистанционного банковского обслуживания или онлайн-банкинг.

Между тем, появление данных сервисов банков значительно усложнило квалификацию хищений, совершаемых в сфере банковского обслуживания. Онлайн-банкинг представляет собой совокупность информационных технологий, направленных на предоставление банковских услуг через сеть Интернет, без личного визита клиента в банк. Наиболее распространенным примером онлайн-банкинга является осуществление банковских операций путем использования телефонов, компьютеров, банкоматов.

В настоящее время можно выделить ряд проблем, возникающих при квалификации хищений данного типа. Прежде всего, какова будет квалификация хищений, совершаемых с использованием данных устройств, если преступник использует одновременно ввод или модификацию компьютерной информации и обман потерпевшего. В данном случае, одна и та же совокупность преступных действий зачастую получает разную уголовно-правовую оценку. К примеру, допустим лицо находит в интернете объявления о продаже имущества, связывается с автором объявлений и убеждает его сообщить номер банковской карты и код доступа. После этого преступник регистрируется в автоматизированных системах от имени владельца карты и получает доступ ко всем счетам потерпевшего. А затем происходит перевод денежных средств со счетов потерпевшего на счета, подконтрольные мошеннику.

Представляется в этой связи, целесообразным сформулировать правила квалификации хищений, совершаемых одновременно путем ввода (модификации) компьютерной информации (статья 278[4] УК) и обмана (п. «в» ч.2 статьи 168 УК), которые позволят разрешить данную проблему.

Полагаем, что разграничение мошенничества и мошенничества в сфере компьютерной информации должно основываться на следующих правилах.

Во-первых, в случаях, когда обман используется лицом для облегчения доступа к чужому имуществу, которое затем похищается другим способом, содеянное не может быть квалифицировано как мошенничество (по статье 168 УК).

Во-вторых, содеянное не может быть квалифицировано как мошенничество также в случае, если получение возможности преступником распоряжаться вещью происходит не в результате обмана.

На основании данных правил представляется необходимым внести ряд уточнений в Постановление Пленума Верховного Суда Республики Узбекистан от 11 октября 2017 года № 35 «О судебной практике по делам о мошенничестве»[1]. Во-первых, необходимо установить, что в случаях, когда обман используется лицом для получения доступа к данным о банковском счете, а имущество похищается путем ввода, модификации компьютерной информации, содеянное следует квалифицировать по совокупности преступлений в виде мошенничества с использованием средств компьютерной техники (п. «в» ч.2 статьи 168 УК), и модификации компьютерной информации (статья 278[4] УК). Во-вторых, следует указать, что если преступник, используя компьютерную информацию (путем отправления через мобильное устройство по мессенджеру Телеграм, электронную почту или иные средства рассылки различных сообщений), приобретает возможность распоряжаться имуществом или имущественными правами потерпевшего непосредственно в результате обмана (например, лицо добровольно перечисляет преступнику денежную сумму), то содеянное необходимо квалифицировать как мошенничество, с учетом размера похищенного имущества по соответствующим частям статьи 168 УК, но без ссылки на п. «в» ч.2 данной статьи, так как мобильное устройство невозможно приравнять к компьютерному средству.

Второй проблемой в сфере квалификации преступлений, совершенных с использованием систем онлайн-банкинга, является квалификация хищений, совершаемых с использованием платежных карт с помощью банкомата. На сегодняшний день они начали получать достаточно заметное распространение. В этой связи в правоприменительный практике и науке стали возникать дискуссии относительно квалификации данных хищений как мошенничества по п. «в» ч.2 ст.168 УК, поскольку банкомат в своей сущности является компьютером.

[1] https://www.lex.uz/docs/3399892.

Вместе с тем, многие отмечают специфику данного мошенничества: воздействие осуществляется на компьютерную информацию, а не на сознание потерпевшего; отсутствует обман лица, отсутствует передача имущества или приобретение права на имущество с помощью потерпевшего; орудием преступления признается информация, средства хранения, передачи и обработки компьютерной информации[2].

Стоит отметить, что, к примеру, в зарубежной судебной практике (Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2007 года № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате») данные хищения квалифицируются как кражи.

Получение кредита в терминале и получение денег в банкомате с помощью поддельной карты имеют общую черту – отсутствие обманных действий, присущих мошенничеству. Поэтому для квалификации получения кредита путем использования чужого паспорта, с которого терминалом автоматически снимается копия, не может использоваться п. «в» ч.2 ст. 168 УК РФ. Данные действия содержат скорее признаки кражи и должны оцениваться в силу их тождественности так же, как и хищение денежных средств в банкомате путем использования поддельной кредитной карты.

Вряд ли можно признать обоснованной различную квалификацию хищения кредита в виде наличных денежных средств и наличных денежных средств из банкомата, если в обоих случаях контрагентом в сделке выступал компьютер, а не уполномоченное организацией лицо, введенное в заблуждение действиями субъекта, а предметом преступления выступали наличные денежные средства.

Вместе с тем, полагаем, что действия подсудимого, осуществляющего установку специальных технических устройств на банкомат, с последующим хищением средств с банковской карты (путем считывания информации, кодов и паролей карты) должны быть квалифицированы не только по п. «б» ч.3 статьи 169 УК (с несанкционированным проникновением в компьютерную систему), но также и по ст.278[2] УК (Незаконный (несанкционированный) доступ к компьютерной информации), поскольку в диспозиции статьи говорится помимо прочего о «перехвате информации».

В качестве решения указанных проблем предлагаем внести изменения в Пленума Верховного Суда Республики Узбекистан от 11 октября 2017 года № 35 «О судебной практике по делам о мошенничестве» и изложить пункт 20 Постановления в следующей редакции:

«20. Разъяснить, что под мошенничеством с использованием средств компьютерной техники (пункт «в» части второй статьи 168 УК) понимается хищение путем обмана чужого имущества, находящегося в

[2] Третьяк М.И. Правила квалификации компьютерного мошенничества и преступлений, предусмотренных гл. 28 УК РФ // Уголовное право, 2014. – № 4 // СПС «Консультант Плюс».

финансовых, банковских учреждениях, фондах и т.п. посредством манипуляций, совершаемых с помощью средств компьютерной техники. Такое мошенничество может быть совершено как путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на соответствующих носителях или передаваемой по сетям передачи данных, так и путем введения в компьютерную систему финансовых, банковских учреждений ложной информации.

В случае, когда обман используется лицом для получения доступа к данным о банковском счете, а имущество похищается путем ввода, модификации компьютерной информации, содеянное следует квалифицировать по совокупности преступлений в виде мошенничества с использованием средств компьютерной техники (п. «в» ч.2 статьи 168 УК), и модификации компьютерной информации (статья 278^4 УК).

Вместе с тем, если преступник, используя компьютерную информацию (путем отправления через мобильное устройство по мессенджеру Телеграм, электронную почту или иные средства рассылки различных сообщений), приобретает возможность распоряжаться имуществом или имущественными правами потерпевшего непосредственно в результате обмана (например, лицо добровольно перечисляет преступнику денежную сумму), то содеянное необходимо квалифицировать как мошенничество, с учетом размера похищенного имущества по соответствующим частям статьи 168 УК, без ссылки на п. «в» ч.2 данной статьи.

Действия виновного, осуществляющего установку специальных технических устройств на банкомат, с последующим хищением средств с банковской карты (путем считывания информации, кодов и паролей карты) должны быть квалифицированы по п. «б» ч.3 статьи 169 УК (с несанкционированным проникновением в компьютерную систему), а также по ст.278^2 УК (Незаконный (несанкционированный) доступ к компьютерной информации)».

На наш взгляд, внесение данных уточнений при отсутствии на настоящий момент профильных статей по киберхищениям в УК Узбекистана, может оказать содействие правоохранительным органам и судам в единообразной и правильной квалификации подобного рода новейших видов хищений.

Библиографические ссылки:

1. Постановление Пленума Верховного Суда Республики Узбекистан от 11 октября 2017 года № 35 «О судебной практике по делам о мошенничестве»

2. Третьяк М.И. Правила квалификации компьютерного мошенничества и преступлений, предусмотренных гл. 28 УК РФ // Уголовное право, 2014. – № 4 // СПС «Консультант Плюс».