Ногинов Владислав Олегович
консультант
АНО «Ярославское правовое научно-исследовательское общество»
Воробьева Анна Николаевна
студентка
ФГБОУ ВО «Ярославский государственный
университет им. П.Г. Демидова»
Засеева Дарья Дмитриевна
студентка
ФГБОУ ВО «Ярославский государственный
университет им. П.Г. Демидова»
г. Ярославль, Ярославская область

ПРОБЛЕМЫ ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ ПРИ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА В СФЕРЕ ОБОРОТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация*: статья посвящена дискуссионным аспектам правоприменительной практики по делам о компьютерном мошенничестве (ст. 159.6 УК РФ). Авторы рассматривают различные варианты оценки отдельных признаков состава анализируемого преступления, исследуют вопросы разграничения со смежными нормами.*

Ключевые слова*: уголовная ответственность, преступление, обман, злоупотребление доверием, компьютерное мошенничество.*

Основная доля компьютерных мошенничеств совершается дистанционно, что затрудняет определение конкретного места совершения преступления. Формально местом совершения киберпреступления, является место, в котором деяние окончено или пресечено, либо место наступления общественно опасных последствий. На практике необходимо устанавливать территориальную подследственность рассмотрения уголовных дел. Традиционно в уголовном праве местом совершения преступления является место, где реализуется объективная

сторона посягательства. Местом совершения мошенничества, как хищения, является место противоправного изъятия имущества у потерпевшего. В пункте 5 ППВС РФ №48 «О судебной практике по делам о мошенничестве, присвоении и растрате» указывается, что мошенничество признается оконченным с момента, когда указанное имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность (в зависимости от потребительских свойств этого имущества) пользоваться или распорядиться им по своему усмотрению. Если предметом являются безналичные денежные средства, в том числе электронные, то такое преступление следует считать оконченным с момента изъятия денежных средств с банковского (или иного) счета, в результате которого владельцу причинен ущерб. Отсюда местом окончания мошенничества в отношении безналичных денежных средств, является место нахождения подразделения банка или иной организации, в котором владельцем был открыт банковский счет или велся учет электронных денежных средств без открытия счета. Значит может возникнуть ситуация, когда подразделение банка расположено на территории одного субъекта РФ, а большинство свидетелей, преступник, потерпевший проживают на территории другого субъекта. В таком случае, согласно ст. 35 УПК РФ, есть основания для изменения территориальной подсудности. Однако подобные ситуации затягивают, затрудняют оперативное рассмотрение уголовных дел, что оказывает негативное воздействие на уголовное судопроизводство.

В доктрине указывается, что компьютерное мошенничество достаточно специфично по отношению к общему составу. Однако, в диспозиции статьи законодателем в качестве способа совершения преступления не указан такой способ, как обман или злоупотребление доверием, что позволяет сделать вывод о том, что состав совершения мошенничества в сфере компьютерной информации не находится в соотношении с составом «классического» мошенничества, а представляет собой самостоятельную форму хищения с присущим ему специфичным, особым способом, отличным и от иных форм хищения чужого имущества [1, с. 563]. Необходимо учитывать, что рассматриваемое преступление лишено

способа совершения, который присущ остальным видам мошенничества – обмана или злоупотребление доверием. В статье не упомянуты ранее названные способы. Соответственно, они являются необязательными признаками объективной стороны мошенничества в сфере компьютерной информации. Внесенные в апреле 2018 г. изменения в ст. 159.3 УК РФ, расширившие способ совершения преступления, порождают конкуренцию с нормой, предусмотренной ст. 159.6 УК РФ. Ранее хищения с использованием систем под общим названием «интернет-банк» квалифицировались по ст. 159.6 УК РФ. Это создает проблемы квалификации данных преступлений. Наиболее часто на практике встречаются случаи, когда содеянное переквалифицируется со ст. 159.6 на п. «г» ч. 3 ст. 158 УК РФ. Объектом этих преступлений является право собственности. Предметом кражи является чужое имущество, а мошенничества в сфере компьютерной информации- чужое имущество или право на чужое имущество. Оба состава являются по своей конструкции материальными. Соответственно, в этой части различий нет. Отличие рассматриваемых составов преступлений заключается в способе их совершения. Так кража определяется как тайное хищение именно имущества Таким определением охватывается посягательство на любую форму собственности и подчеркивается, что имущество является для похитителя чужим [2, с. 21].

В пункте 2 ППВС РФ №29 «О судебной практике по делам о краже, грабеже и разбое» сказано, что «как тайное хищение чужого имущества (кража) следует квалифицировать действия лица, совершившего незаконное изъятие имущества в отсутствие собственника или иного владельца этого имущества, или посторонних лиц либо хотя и в их присутствии, но незаметно для них. В тех случаях, когда указанные лица видели, что совершается хищение, однако виновный, исходя из окружающей обстановки, полагал, что действует тайно, содеянное также является тайным хищением чужого имущества». Тайность означает, что изъятие и обращение имущества происходят скрытно, незаметно для собственника или иного владельца либо других лиц. Эти лица либо не видят действий виновного, либо не осознают их противозаконности [3]. В случае мошенничества в сфере компьютерной информации хищение совершается путем ввода, удаления,

блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Согласно п. 21 ППВС РФ №48, совершаемое путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т. п.), такие действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. При этом изменение данных о состоянии банковского счета и (или) о движении денежных средств, происшедшее в результате использования виновным учетных данных потерпевшего, не может признаваться таким воздействием [3].

Необходимо обратить внимание, что телефоном, планшетом или иным устройством, к которому подключена услуга «мобильный банк» злоумышленник может завладеть тайно либо путем обмана. Соответственно, могут присутствовать признаки кражи или мошенничества. Учитывая, что изменение данных о состоянии банковского счета и (или) о движении денежных средств, происшедшее в результате использования виновным учетных данных потерпевшего не рассматривается в качестве незаконного воздействия на программное обеспечение, то целесообразно квалифицировать содеянное как кражу. Стоит отметить, что совершение хищения путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей не исключает тайности деяния [3].

Основными отличиями кражи от мошенничества являются: при мошенничестве преступник действует открыто, при краже – тайно; при мошенничестве злоумышленник путем обманных действий вынуждает потерпевшего совершить действия, результатом которых будет изъятие имущества, в частности денежных

средств, при краже потерпевший не принимает участие в процессе, ведущим к изъятию имущества, денежных средств. В тех случаях, когда виновный тайно либо путем обмана воспользовался телефоном потерпевшего, автоподключением к услуге «мобильный банк», авторизовался в системе интернет-платежей под известным ему данными другого лица и т. п., такие действия подлежат квалификации как кража (ст.158 УК РФ) [3].

Список литературы

1. Соловьев О.Г. Дискуссионные аспекты конструирования составов преступлений в сфере экономической деятельности (гл. 22 УК РФ) / О.Г. Соловьев // Вестник Ярославского государственного университета им. П.Г. Демидова. Серия Гуманитарные науки. – 2021. – Т. 15. №4. – С. 560–567.

2. Грузинская Е.И. К вопросу о разграничении дифференциации и индивидуализации в уголовном праве / Е.И. Грузинская, Ю.О. Авдеева // Актуальные вопросы борьбы с преступлениями. – 2016. – №1. – С. 21–23.

3. Арутюнов А.А. Преступления против собственности/ А.А. Арутюнов [Электронный ресурс]. – Режим доступа: https://viperson.ru/articles/prestupleniya-protiv-sobstvennosti (дата обращения 10.02.2023).