

© Екатерина Евгеньевна Чередниченко
кандидат юридических наук, доцент,
доцент кафедры уголовно-правовых дисциплин
Владимирского филиала РАНХиГС,
г. Владимир
Cheredn@mail.ru

Ekaterina E. Cherednichenko
Candidate of Legal Sciences,
Associate Professor,
Associate Professor of the Department of
Criminal Law Disciplines,
Vladimir Branch of the RANEPa,
Vladimir

К ВОПРОСУ ОБ ОБЪЕКТИВНЫХ ПРИЗНАКАХ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

On the issue of objective signs of fraud using electronic means of payment

Аннотация. В представленной статье анализируются объективные признаки состава преступления, предусматривающего уголовную ответственность за мошенничество с использованием электронных средств платежа. Автор рассматривает объект, предмет и объективную сторону, указывает на существующие проблемы в теории и на практике, называет способы совершения такого вида мошенничества.

Annotation. The presented article analyzes the objective features of the composition providing for criminal liability for fraud using electronic means of payment. The author examines the object, the subject and the objective side, points out the existing problems in theory and in practice, and names ways to commit this type of fraud.

Ключевые слова: мошенничество, обман, злоупотребление доверием, электронные средства платежа.

Keywords: fraud, deception, abuse of trust, electronic means of payment.

Общий ущерб, нанесенный россиянам со стороны IT-мошенников, в 2024 году превысил 170 млрд. рублей. Об этом сообщил в ходе пресс-конференции, посвященной Всемирному дню безопасного интернета, член Комитета Госдумы по информационной политике, информационным технологиям и связи Антон Немкин [5]. Глава МВД России Владимир Колокольцев указал, что пострадавшими от незаконных действий в цифровой сфере становятся физические и юридические лица, в том числе государственные структуры. Киберпреступлениями наносится существенный вред экономике и имущественным правам граждан [8].

Уголовный кодекс РФ в качестве одной из своих задач называет предупреждение преступлений. Но для выполнения этой задачи необходимо понимать, в чем же суть каждого из видов преступлений.

Традиционно анализ состава любого преступления начинается с характеристики объекта, потому что именно он представляет собой те общественные отношения, которые охраняются данной уголовно-правовой нормой. Понимание объекта преступления позволяет правильно

квалифицировать деяние и определить его общественную опасность, что является основой для применения соответствующих мер уголовной ответственности.

Кроме того, объект преступления напрямую связан с оценкой причиненного ущерба. Это важно для установления наличия или отсутствия состава преступления, так как некоторые преступления требуют обязательного наличия ущерба для признания их таковыми. Анализ объекта преступления помогает различать составы преступлений, которые могут иметь схожие объективные стороны, но направлены на разные объекты.

Понимание объекта преступления позволяет точнее определить субъективную сторону преступления, установить мотивы и цели. Это важно для полноценной характеристики преступного деяния и назначения справедливого наказания. Кроме этого информация об объектах преступлений помогает разрабатывать и внедрять эффективные меры по предупреждению преступлений и защите общественных отношений.

Таким образом, характеристика объекта преступления является отправной точкой для всестороннего анализа состава преступления, что позволяет обеспечить правильное правоприменение, защиту общественных интересов и разработку эффективных мер профилактики преступлений.

Уголовная ответственность за мошенничество с использованием электронных средств платежа регламентируется статьей 159.3 главы 21 «Преступления против собственности» раздела VIII «Преступления в сфере экономики» Уголовного кодекса Российской Федерации. Из этого следует, что родовым объектом данного вида мошенничества являются общественные отношения, регулирующие экономическую сферу. Видовым объектом являются общественные отношения, охраняющие право собственности.

Понимание права собственности включает несколько подходов, отражающих разные аспекты и функции этого правового института. Основные подходы к пониманию права собственности включают юридический, экономический, философский и социологический аспекты.

С юридической точки зрения право собственности представляет собой совокупность правомочий, которыми владеет собственник по отношению к своему имуществу. Это право обычно включает три ключевых компонента: право владения, право пользования и право распоряжения.

Итак, владение – это фактическое обладание имуществом и возможность физического контроля над ним. Владение может быть законным, если оно основано на праве, и незаконным, если происходит вопреки правовым нормам; пользование – это возможность извлекать полезные свойства из имущества, то есть использовать его в своих интересах. Пользование может включать как личное использование, так и сдачу имущества в аренду; и наконец, распоряжение – это право определять юридическую судьбу имущества, например, путем его продажи, дарения, завещания или передачи в наследство. Распоряжение также включает в себя возможность обременения имущества, например, путем его залога.

Предметом мошенничества выступает имущество или право на

имущество [1, с. 146]. Это приводит к спорам о том, как понимать и описывать данное преступление. Некоторые считают, что уголовная ответственность за мошенничество включает два отдельных состава, различаемых по объекту [7]. Иные специалисты высказывают идею об отделении мошенничества от хищения из-за возможности совершения преступных действий не только в отношении конкретного имущества, но и в отношении имущественных прав [2].

Также возникает сомнение в основном критерии предмета хищения, который многие исследователи определяют как физический или материальный аспект имущества [3, с. 50].

Физический аспект, безусловно, играет значительную роль, но он не является единственным критерием. В действительности, предмет похищения может включать в себя не только материальные вещи, но и нематериальные ценности, которые имеют экономическую стоимость. Рассмотрим этот вопрос подробнее. Предмет хищения действительно часто имеет физический аспект. Это означает, что объект является материальной вещью, которую можно физически изъять и присвоить. К таким объектам относятся:

- наличные деньги – их можно физически забрать у владельца;
- техника и электроника – мобильные телефоны, ноутбуки, телевизоры и т.д.;
- автомобили – транспортные средства, которые можно угнать или похитить.

Предметом хищения могут быть и нематериальные ценности. Это объекты, которые не имеют физической формы, но обладают экономической ценностью и могут быть присвоены. К таким объектам относятся:

- денежные средства на счетах – хотя физически они не существуют, их можно перевести и присвоить и они представляют реальную ценность;
- ценные бумаги и акции – электронные записи о правах на долю в компании, которые имеют рыночную стоимость;
- интеллектуальная собственность – патенты, авторские права, торговые марки и коммерческая тайна;
- данные и информация – базы данных, персональные данные клиентов, которые можно использовать в корыстных целях.

В условиях бурно развивающегося мира, где множество предметов материального мира переходят в цифровое пространство, физический признак предмета хищения постепенно теряет свою актуальность. Традиционно хищение ассоциировалось с присвоением материальных объектов: денег, ювелирных изделий, автомобилей и других вещей, обладающих физическими характеристиками. Однако с появлением и широким распространением электронных средств платежа, криптовалют и других нематериальных активов границы этого понятия значительно расширились.

Одним из ярких примеров устаревания физического признака предмета хищения является кража денежных средств с банковских счетов посредством взлома компьютерных систем. В таких случаях преступник не получает в руки

физические деньги, но тем не менее совершает хищение. Средства переводятся на другие счета, используемые для последующего обналичивания или дальнейших преступных операций. Важным здесь является факт нарушения имущественных прав, а не физическое обладание предметом преступления.

Помимо постоянных случаев краж безналичных денежных средств и цифровых валют все чаще встречаются случаи краж виртуальных активов граждан, таких как персональные аккаунты и виртуальные объекты в компьютерных играх или приложениях, которые были приобретены за реальные деньги. Так, сотрудники полиции Нижегородской области раскрыли кражу танка в игре World of Tanks. Личность злоумышленника установили, когда он пытался перепродать чужой аккаунт за реальные деньги [4].

Все это вызывает активные дискуссии среди юристов о возможности внесения законодательных изменений для установления уголовной ответственности за кражу виртуальных активов [6]. А. В. Шульга [9, с. 11] обращает внимание на то, что традиционное понимание предмета преступлений против собственности уже не отражает современные общественные отношения. Исследователь подчеркивает, что важными критериями для определения предмета посягательства следует считать не только его материальную природу и создание человеческим трудом, но и его реальную или потенциальную коммерческую ценность, способность быть товаром и участвовать в законном экономическом обороте.

Таким образом, предмет хищения включает следующие аспекты:

- возможность присвоения - предмет должен быть таким, чтобы его можно было изъять и присвоить;
- незаконность изъятия - изъятие должно быть незаконным, то есть без согласия собственника;
- имущественный характер - предмет должен быть частью имущественного оборота и иметь экономическую стоимость.

Объективная сторона состава преступления, предусмотренного ст. 159.3 УК РФ, включает в себя три элемента: деяние в виде мошенничества, совершенного путем обмана или злоупотребления доверием, последствия в виде причиненного ущерба и причинно-следственная связь.

Мошенничество с использованием электронных средств платежа включает в себя различные схемы, суть которых сводится к незаконному присвоению денежных средств посредством цифровых технологий. Вот основные этапы, которые могут присутствовать в таком виде мошенничества:

1) фишинг – создание поддельных веб-сайтов или отправка электронных писем и сообщений, которые имитируют официальные запросы от банков или платежных систем. Цель – обманом заставить пользователя ввести свои учетные данные, такие как логин и пароль;

2) скимминг – установка специальных устройств на банкоматах или платежных терминалах, которые считывают данные с магнитной полосы карты. Дополнительно могут использоваться скрытые камеры для записи PIN-кодов;

3) вишинг – звонки по телефону от лица, представляющегося сотрудником банка или платежной системы, с целью получения конфиденциальной информации, такой как номер карты, CVV-код, пароли и коды подтверждения;

4) малварь – распространение вредоносных программ, которые заражают устройства пользователя и могут перехватывать данные вводимых паролей или автоматически проводить несанкционированные транзакции;

5) социальная инженерия – использование психологических методов для манипулирования людьми и получения от них конфиденциальной информации. Мошенники могут, например, создавать ложные ситуации срочности (родственник попал в аварию) или угрожать, заставляя жертву действовать необдуманно;

6) взлом учетных записей – кража логинов и паролей с последующим доступом к банковским или платежным аккаунтам жертвы, что позволяет совершать несанкционированные переводы и покупки.

Однако следует сказать, что этот перечень со временем только расширяется, появляются новые способы обмана и злоупотребления доверием. Основная проблема, которая существует сегодня, по нашему мнению, сводится к тому, что правоохранительные органы не могут предотвратить мошенничества в силу их быстрой трансформации и появления новых возможностей для лиц, желающих незаконно обогатиться.

В настоящее время принят целый ряд законодательных норм, направленных на противодействие мошенническим действиям, вместе с тем без активной работы с населением, юридическими лицами невозможно добиться положительных результатов. Полагаем, что работа в данной сфере должна носить комплексный характер и включать в себя различные меры в разных сферах общественной жизни.

Список литературы

1. Карпова Н. А., Калининская Я. С. Уголовно-правовая характеристика и проблемы квалификации мошенничества с использованием платежных карт // Проблемы экономики и юридической практики. – 2017. – № 5. – С. 145-147.

2. Корепанова Е. А. К вопросу о безналичных денежных средствах как предмете преступлений // Пробелы в российском законодательстве. – 2017. – № 6. – С. 24-28.

3. Лопашенко Н. А. Посягательства на собственность. – М., 2012. – 527 с.

4. Нижегородский угрозыск обнаружил танк, «угнанный» в онлайн-игре // Информационный ресурс Newsnn.ru : [сайт]. URL: <https://newsnn.ru/news/society/02-03-2016/nizhegorodskiy-ugrozyskobnaruzhil-tank-ugnannyy-v-onlayn-igre> (дата обращения: 23.03.2024).

5. Общий ущерб россиянам от IT-мошенников превысил 170 млрд рублей // ComNews.ru : [сайт]. URL: <https://www.comnews.ru/content/237738/2025-02-12/2025-w07/1009/obschiy->

uscherb-rossiyanam-it-moshennikov-prevysil-170-mlrd-rublej (дата обращения: 17.02.2025).

6. Похитители танков. За кражу аксессуаров компьютерных игр будет грозить уголовное наказание // Рос. газ. – 2019. – Федеральный выпуск № 207 (7965). URL: <https://rg.ru/2019/09/16/v-rf-vvedut-ugolovnoe-nakazanie-za-krazhu-predmetov-v-kompiuternyh-igrah.html> (дата обращения: 23.03.2024).

7. Тамазов И. А. Объект и предмет мошенничества // Современное право. – 2010. – № 12. – С. 129-131.

8. Ущерб от IT-мошенничества за 11 месяцев 2024 года составил 168 млрд. рублей // ТАСС : [сайт]. URL: <https://tass.ru/obschestvo/22814225> (дата обращения: 02.02.2025).

9. Шульга А. В. Объект и предмет преступлений, посягающих на собственность в условиях рыночных отношений и информационного общества : автореф. дис. ... д-ра юрид. наук : 12.00.08 / Андрей Владимирович Шульга. – Краснодар, 2009. – 30 с.