4 [2024]
ISBN 978-5-901722-87-9
ТРАНСПОРТ. ГОРИЗОНТЫ РАЗВИТИЯ

УДК 343.3/7

ХИЩЕНИЯ, СОВЕРШАЕМЫЕ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: ВОПРОСЫ КВАЛИФИКАЦИИ

Щеголева Ксения Вячеславовна[1], магистрант
e-mail: rctybz19991@mail.ru

[1] Волжский государственный университет водного транспорта, Нижний Новгород, Россия

Аннотация. В статье рассматриваются типичные ситуации хищения безналичных и электронных денежных средств, а также возникающие проблемы и ошибки при их квалификации. Недостаточное понимание признаков составов преступлений влечет за собой неверную квалификацию деяний. Это свидетельствует о необходимости дальнейшего совершенствования уголовно-правовых норм и исключения некоторых статей из Уголовного кодекса Российской Федерации. Автор статьи высказывает мнение о необходимости увеличения ясности и прозрачности в уголовно-правовой сфере путем введения самостоятельного состава преступления «Хищение с использованием информационных технологий».

Ключевые слова: кража, хищение, электронные денежные средства, информационные технологии, квалификация преступлений, киберпреступность.

THEFT COMMITTED WITH THE USE OF IFORMATION TECHNOLOGIES: QUALIFICATION ISSUES

Shchegoleva Ksenia Vyacheslavovna[1], Master's Degree Student
e-mail: rctybz19991@mail.ru

[1] Volga State University of Water Transport, Nizhny Novgorod, Russia

Abstract. The article considers typical situations of theft of non-cash and electronic money, as well as emerging problems and errors in their qualification. Insufficient understanding of the signs of the elements of offences entails incorrect qualification of acts. This demonstrates the need for further improvement of criminal law norms and exclusion of some articles from the Criminal Code of the Russian Federation. The author of the article expresses an opinion on the need to increase clarity and transparency in the criminal-legal sphere by introducing an independent corpus delicti of the offence «Theft with the use of information technologies».

Keywords: theft, embezzlement, electronic money, information technology, qualification of offences, cybercrime.

Ведение

Цифровизация играет значительную роль в повседневной жизни человека, облегчая и ускоряя решение бытовых и профессиональных задач. Однако, вместе с позитивными

моментами, она также открывает двери для совершения преступлений. Использование цифрового пространства для совершения преступлений становится все более распространенным явлением. Благодаря современным цифровым технологиям преступники находят новые способы совершения преступления, а также обходят законы и контроль со стороны правоохранительных органов. Это создает дополнительные вызовы для современного общества и требует развития новых методов борьбы с цифровой преступностью. Одним из ключевых аспектов при использовании цифровых технологий становится защита личной информации и конфиденциальность. С увеличением количества онлайн-торговли, использования социальных сетей и электронного банкинга, важно обеспечить надежную защиту данных пользователей от потенциальных хакерских атак и киберугроз [1].

В начале 2024 года количество зарегистрированных преступлений в Российской Федерации осталось на уровне января прошлого года, увеличившись всего на 0,2%. Однако число киберпреступлений за этот период увеличилось на 24,4%, что свидетельствует о росте интереса к этому виду преступлений. Преступления, попадающие под статьи 159-159.6 Уголовного кодекса Российской Федерации составляют 22,7% от общего числа зарегистрированных преступлений за январь 2024 года. Это говорит о значительной доле серьезных преступлений в общей структуре преступности в стране [6].

Сегодня киберпреступность продолжает активно развиваться, охватывая все новые области деятельности. Например, мошенничество в сети Интернет, кибершпионаж, кибертерроризм и другие виды преступлений становятся все более распространенными. Как защитить себя от киберугроз? Для защиты от киберугроз необходимо соблюдать меры безопасности в сети, использовать надежные пароли, обновлять программное обеспечение и иметь антивирусное программное обеспечение. Также важно быть внимательным при общении в сети и не разглашать свои личные данные.

Признавая необходимость учета информационных технологий при рассмотрении уголовных дел, следует отметить, что введение новых признаков в составы преступлений может вызывать юридические сложности. Это сложности могут заключаться в неоднозначном определении границ между категориями преступлений, что затрудняет судебное разбирательство и требует от специалистов большей внимательности и точности в квалификации преступлений [3].

На сегодняшний день уголовная ответственность за хищение с использованием информационных технологий регулируется несколькими статьями Уголовного кодекса Российской Федерации. В частности, пункт «г» части 3 статьи 158 УК РФ содержит особо квалифицированный состав преступления – кражу с банковского счета и электронных денежных средств. Также статья 159.3 УК РФ предусматривает ответственность за мошенничество с использованием электронных средств платежа. Рассмотрение уголовных дел о хищении с использованием информационных технологий требует специальных знаний и компетенций в области цифровых технологий и методов определения мошенничества в сети. Материальный улики могут представлять собой различные данные, полученные из компьютерных систем и сетей. Для эффективной борьбы с преступлениями, связанными с использованием информационных технологий, необходимо использовать специализированные методы и технологии, а также современные программные и аппаратные средства для выявления и пресечения незаконных действий. Обучение правоохранительных органов и сотрудников банков в области кибербезопасности также является важным аспектом профилактики и борьбы с преступлениями. Перед внесением изменений в Уголовный кодекс Российской Федерации в 2018 году ст. 159.3 УК РФ имела другое содержание: совершение преступления было связано с обманом сотрудника кредитной, коммерческой или иной организации, а объектом преступления являлась только

платежная карта. Однако Федеральным законом от 23 апреля 2018 года № 111-ФЗ был внесен новый квалифицирующий признак кражи, и ст. 159.3 УК РФ была изменена. Кроме того, ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации» была дополнена новым квалифицирующим признаком, аналогичным тому, который был внесен в состав кражи [2].

Одним из вопросов, возникающих в связи с этим, является соотношение и разграничение составов преступлений. Кража с банковского счета, мошенничество с использованием электронных средств платежа – все это формы хищения, объединенные общим предметом преступления. Все эти действия совершаются с целью личной выгоды и требуют использования современных технологий.

Одним из главных преимуществ электронных денежных средств является повышенный уровень безопасности транзакций. Также использование электронных средств облегчает проведение платежей в любое время и в любом месте, что делает их удобными для потребителей и бизнеса. Для эффективного функционирования электронных денежных средств необходимо соответствующее правовое регулирование. Законы и нормативные акты охраняют интересы пользователей электронных средств, обеспечивая им защиту и гарантии при совершении электронных платежей [4].

Кража характеризуется тем, что вор подходит к совершению преступления скрытно, без налицо явного намерения. Он старается совершить кражу таким образом, чтобы его действия не вызывали подозрений у потерпевшего и окружающих. Мошенничество, напротив, связано с обманом других лиц или злоупотреблением их доверием. Основой для совершения мошенничества может выступать ложь, манипуляции или другие уловки, направленные на личную выгоду виновного лица. Таким образом, хотя и кража, и мошенничество относятся к преступлениям против имущества, их способы совершения и характеристики значительно отличаются друг от друга. Важно различать эти виды преступлений, чтобы эффективно бороться с преступностью и защищать права граждан.

В соответствии с разъяснениями Пленума Верховного Суда Российской Федерации, статья 159.6 УК РФ применяется при целенаправленном воздействии программных или программно-аппаратных средств на серверы, компьютеры или информационно-телекоммуникационные сети, нарушающем процесс обработки, хранения, передачи компьютерной информации.

Появление новых устройств способствует увеличению безопасности и удобства при совершении платежей. В будущем количество доступных способов оплаты будет увеличиваться, открывая новые перспективы для потребителей. Прогресс в области безналичных платежей способствует распространению использования электронных средств оплаты в повседневной жизни. Электронные кошельки, мобильные приложения и другие технологии делают процесс оплаты более удобным и быстрым. Эти инновации предоставляют новые возможности как для потребителей, так и для компаний, стремящихся быть впереди времени и обеспечить клиентов наилучшими условиями.

Существует несколько ключевых типов киберпреступлений, которые по своей сложности могут считаться особыми и сложными для идентификации. Для эффективного противодействия и раскрытия киберпреступлений необходимо разработать эффективные подходы и стратегии борьбы с данным видом преступлений.

В первую очередь, преступник прибегает к использованию поддельных или украденных банковских карт, чтобы получить доступ к чужим денежным средствам. При этом он предоставляет ложные данные или умалчивает о том, что не имеет права на использование данной карты. Таким образом, мошенник завладевает средствами других лиц. Важно не передавать данные карты третьим лицам, не использовать не свои карты для оплаты товаров

и услуг, а также вовремя блокировать карту в случае ее утери или кражи. Только совместными усилиями можно минимизировать риски попадания в ловушку мошенников.

Платежная карта является электронным средством платежа, позволяя совершать операции без необходимости физического контакта. С развитием технологий сейчас стало возможным осуществлять бесконтактные платежи, что делает использование платежных карт еще более удобным и безопасным. При использовании электронных средств платежа, в том числе платежных карт, важно помнить о соблюдении законодательства. В случае использования карты без предъявления документа, удостоверяющего личность, владелец карты не вводит продавца в заблуждение, однако вопросы могут возникнуть при определении истинного владельца карты и легальности операции. Бесконтактный метод оплаты обеспечивает не только удобство, но и повышенный уровень безопасности при совершении платежей. Важно быть внимательным и осторожным, чтобы избежать возможных недоразумений и конфликтов при использовании электронных средств платежа.

Во-вторых, важно отметить, что недобросовестные личности могут использовать поддельные или украденные платежные карты для снятия чужих средств через банкомат. Подобные действия рассматриваются как кража. В современных условиях необходимо также учитывать отношение к электронным средствам платежа. К примеру, согласно ч. 3 ст. 158 УК РФ, хищение денег через банкомат может рассматриваться как тяжкое преступление в больших размерах, что подчеркивает значимость борьбы с подобными преступлениями в обществе. По закону, максимальное наказание за хищение по пункту «г» части 3 статьи 158 УК РФ составляет 6 лет лишения свободы.

Преступления, связанные с завладением чужими средствами, могут иметь различные квалификации. Некоторые действия не всегда могут рассматриваться как кража, если учетные данные были использованы для осуществления операции в присутствии третьих лиц.

По мнению Верховного Суда Российской Федерации, действия виновного, который обманом переводит деньги со счета потерпевшего на свою карту, подпадают под состав кражи. Даже если владелец устройства был обманут, это не освобождает персону от ответственности. Мошенничество в области компьютерной информации часто сопровождается «компьютерной кражей». Главное различие между этими понятиями заключается в способе совершения преступления. Если виновный применяет метод, который можно назвать «компьютерным взломом», это позволяет квалифицировать его действия как мошенничество.

Разъяснения высшей судебной инстанции до сих пор не решили трудности в определении хищений безналичных, включая электронные, денежных средств. Используя интернет-технологии, можно чужими деньгами различными способами. Таким образом, требуется усовершенствовать законодательство для более эффективной борьбы с хищениями безналичных средств. Необходимо разработать новые нормы, учитывающие современные методы мошенничества, чтобы обеспечить защиту финансовых интересов граждан и компаний. Кроме того, важно проводить профилактическую работу и информировать население о возможных способах мошенничества с использованием безналичных средств. Обучение граждан основам финансовой безопасности и соблюдение мер предосторожности могут значительно снизить риски утраты денежных средств.

В настоящее время четкое разграничение между различными видами мошенничества становится все более проблематичным. Это относится к краже с банковского счета или электронных денежных средств, мошенничеству с использованием электронных средств платежа и мошенничеству в сфере компьютерной информации. Для эффективного противодействия современным видам мошенничества необходима разработка новых

стратегий и мер борьбы. Учитывая развитие технологий и переход многих операций в онлайн-режим, важно создать механизмы, позволяющие эффективно защищать банковские счета и электронные денежные средства от злоумышленников. Также необходимо улучшить законодательную базу и повысить информированность граждан о возможных угрозах. Одним из ключевых моментов в борьбе с мошенничеством является образование и просвещение населения. Граждане должны быть информированы о методах защиты своих финансовых данных, понимать возможные угрозы и уметь реагировать на них. Такой подход поможет снизить вероятность столкновения с мошенниками и повысит уровень безопасности в целом.

Важным аспектом борьбы с преступностью является единообразное понимание и квалификация преступлений. Для повышения эффективности деятельности правоохранительных органов предлагается исключить из Уголовного кодекса Российской Федерации некоторые статьи, такие как часть 3 статьи 158, статья 159.3 и статья 159.6. Кроме того, предлагается ввести новый состав преступления под названием «Хищение с использованием информационных технологий», который объединит различные формы хищения с помощью современных технологий. Это позволит более эффективно пресекать преступления и предотвращать их совершение в будущем [5].

Список литературы:

1. Шестало С.С. Новое в уголовном законодательстве о хищении безналичных денежных средств // Юрист. 2018. № 8. С. 39 – 44. – URL: https://old.lawinfo.ru/assets/files/Lawyer/2018/8/Lawyer_8_18-7.pdf (дата обращения: 04.03.2024)
2. Архипов А.В. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства // Уголовное право. 2018. № 3. С. 4 – 9. – URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=115691#WrdOYCUWM1vq2oO51 (дата обращения: 04.03.2024)
3. Яни П. С. Мошенничество с использованием электронных средств платежа // Законность. 2019. № 4. С. 30 – 35. – URL: https://www.elibrary.ru/ip_restricted.asp?rpage=https%3A%2F%2Fwww%2Eelibrary%2Eru%2Fitem%2Easp%3Fid%3D39537076 (дата обращения: 05.03.2024)
4. Хисамова З.И. Об уголовной ответственности за хищения, совершенные с использованием IT-технологий: анализ изменений законодательства и правоприменительной практики // Российский следователь. 2018. № 9. С. 43 – 47. – URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=117545#upoPYCUqUFarS0ao (дата обращения: 05.03.2024)
5. Шарапов, Р.Д. Постановление Пленума Верховного Суда России «О судбеной практике по делам о мошенничестве, присвоении и растрате»: заметки на полях // Криминалистъ. 2018. № 4. С. 16-22. – URL: https://cyberleninka.ru/article/n/postanovlenie-plenuma-verhovnogo-suda-rossii-o-sudebnoy-praktike-po-delam-o-moshennichestve-prisvoenii-i-rastrate-zametki-na-polyah (дата обращения: 06.03.2024)
6. Краткая характеристика состояния преступности в Российской Федерации за январь 2024 года // МВД России: официальный сайт. – URL: https://мвд.рф/reports/item/47525142/ (дата обращения: 02.03.2024)