УДК 343.98

НАУЧНЫЙ ЖУРНАЛ
«БИЗНЕС И ОБЩЕСТВО»

Акиньшина Мария Сергеевна
студент магистратуры
Московский университет им. С.Ю. Витте
Москва, Россия

ОСОБЕННОСТИ ВЫЯВЛЕНИЯ И РАССЛЕДОВАНИЯ ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ПЛАСТИКОВЫХ КАРТ

Аннотация

Рассматриваются особенности выявления и расследования хищений денежных средств, совершаемых с использованием пластиковых карт и электронных средств платежа. Проанализированы основные способы совершения преступлений в данной сфере, исследованы проблемы, возникающие при раскрытии и расследовании подобных деяний, а также рассмотрены особенности проведения отдельных следственных действий. Особое внимание уделено вопросам использования специальных знаний, цифровых следов и взаимодействия правоохранительных органов с банковскими организациями. Сделан вывод о необходимости совершенствования криминалистической методики расследования преступлений, связанных с использованием банковских карт.

Ключевые слова: банковская карта, хищение денежных средств, мошенничество, криминалистика

Современная финансовая система Российской Федерации характеризуется активным развитием безналичных расчетов и широким использованием электронных средств платежа. Банковские карты стали неотъемлемой частью повседневной жизни населения, поскольку используются при получении заработной платы, социальных выплат, оплате товаров и услуг, а также при дистанционном осуществлении финансовых операций. Одновременно с этим наблюдается устойчивый рост преступлений, связанных с неправомерным использованием пластиковых карт и их реквизитов. Расширение цифровой среды привело к возникновению новых способов противоправного завладения денежными средствами, что обусловило необходимость совершенствования механизмов выявления и расследования подобных деяний [2].

В соответствии с положениями Федерального закона «О национальной платежной системе» электронным средством платежа признается средство или способ, позволяющий клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения для осуществления перевода денежных средств [2]. На практике это означает, что банковская карта представляет собой не только инструмент осуществления расчетов, но и средство удаленного доступа к банковскому счету. Подобная особенность существенно повышает уязвимость граждан перед преступными посягательствами, совершаемыми с использованием современных информационных технологий.

Следует отметить, что преступления данной категории отличаются высокой степенью общественной опасности. Денежные средства могут быть похищены дистанционно, без непосредственного контакта преступника с потерпевшим. Значительная часть подобных преступлений совершается с использованием методов социальной инженерии, фишинговых ресурсов, вредоносного программного обеспечения, а также специализированных технических устройств, предназначенных для копирования данных банковских карт. Подобные действия зачастую квалифицируются по статьям УК РФ, предусматривающим ответственность за кражу либо мошенничество с использованием электронных средств платежа [1].

Особое значение для правильной квалификации преступлений имеет разграничение мошенничества с использованием электронных средств платежа и смежных составов преступлений. Как отмечают А. В. Воробьева и Н. А. Кудрявцева, в правоприменительной практике нередко возникают сложности при определении способа совершения преступления и характера действий виновного лица. Ошибки квалификации могут быть связаны с тем, что преступления данной категории одновременно содержат признаки хищения денежных средств, незаконного доступа к информации и использования электронных технологий [4].

Одной из наиболее распространенных схем совершения преступлений остается телефонное мошенничество. Преступники представляются сотрудниками банковских организаций, правоохранительных органов либо государственных учреждений и убеждают потерпевших самостоятельно сообщить реквизиты банковских карт, коды подтверждения операций или перевести денежные средства на подконтрольные счета. В подобных ситуациях преступное воздействие строится преимущественно на психологическом давлении, создании чувства опасности либо срочности совершаемых действий. Потерпевший, находясь в стрессовой ситуации, самостоятельно предоставляет преступникам доступ к своим денежным средствам.

Не менее распространенным способом совершения преступлений является использование скимминговых устройств. Сущность данного метода заключается в незаконном копировании сведений с магнитной полосы банковской карты. Для этого преступники устанавливают на банкоматы специальные накладки, позволяющие считывать информацию о карте, а также устройства для фиксации ПИН-кода. Полученные сведения используются для изготовления дубликатов банковских карт и последующего снятия денежных средств со счетов потерпевших [6].

Развитие интернет-технологий привело к увеличению количества преступлений, связанных с использованием фишинговых сайтов и вредоносного программного обеспечения. Потерпевший, переходя по поддельной ссылке или устанавливая зараженное приложение, самостоятельно передает злоумышленникам конфиденциальную информацию. В результате преступники получают возможность осуществлять дистанционный доступ к банковским счетам граждан и совершать несанкционированные операции.

Особенность расследования рассматриваемой категории преступлений заключается в необходимости работы с цифровыми следами. Практически каждая операция, связанная с переводом денежных средств, сопровождается фиксацией технической информации: IP-адресов, номеров телефонов, сведений о банковских счетах, данных устройств, с которых осуществлялся вход в систему дистанционного банковского обслуживания. Именно поэтому расследование подобных преступлений требует активного использования специальных знаний в области информационных технологий [5].

Выявление преступлений чаще всего начинается с обращения потерпевшего в банковскую организацию либо правоохранительные органы после обнаружения факта незаконного списания денежных средств. На первоначальном этапе расследования особое значение имеет своевременное получение информации о движении денежных средств, а также принятие мер, направленных на их блокировку. Следователю необходимо установить время и способ совершения операций, маршруты движения денежных средств, сведения о лицах, на счета которых были осуществлены переводы.

Как справедливо отмечают Е. В. Безручко и А. А. Романенко, значительные сложности возникают при расследовании преступлений, совершаемых с использованием эквайрингового оборудования. Преступники могут использовать поддельные терминалы оплаты, фиктивные торговые точки либо измененное программное обеспечение, что требует проведения сложных технических исследований и привлечения специалистов в области банковских технологий [3].

Важным элементом расследования является проведение следственного осмотра. Объектами осмотра могут выступать банкоматы, POS-терминалы, банковские карты, мобильные устройства, компьютерная техника и документы, содержащие сведения о банковских операциях. Особое внимание уделяется обнаружению

технических устройств, следов вмешательства в программное обеспечение, а также фиксации цифровой информации, способной иметь доказательственное значение.

Существенную роль в расследовании рассматриваемых преступлений играет взаимодействие правоохранительных органов с кредитными организациями. Банки располагают сведениями о движении денежных средств, способах авторизации операций, местоположении банкоматов и терминалов, а также иной информацией, имеющей значение для уголовного дела. Оперативное получение таких данных позволяет своевременно установить обстоятельства совершения преступления и определить направление дальнейшего расследования [6].

Особое значение имеет производство судебных экспертиз. Наиболее востребованными являются компьютерно-технические, дактилоскопические, фоноскопические и почерковедческие исследования. Компьютерно-техническая экспертиза позволяет исследовать электронные устройства, установить наличие вредоносного программного обеспечения, определить способы получения несанкционированного доступа к банковским системам и восстановить удаленную информацию.

Сложности при расследовании преступлений данной категории нередко связаны с трансграничным характером совершаемых деяний. Денежные средства могут переводиться через несколько банковских счетов, оформленных на подставных лиц, а сами преступники зачастую находятся за пределами Российской Федерации. Подобные обстоятельства требуют активного международного взаимодействия правоохранительных органов и использования современных механизмов обмена информацией.

Пленум Верховного Суда Российской Федерации неоднократно обращал внимание на необходимость правильного разграничения кражи и мошенничества в отношении денежных средств, находящихся на банковских счетах. Как отмечает А. К. Князькина, правильная квалификация преступления имеет принципиальное значение для определения характера противоправных действий и установления способа совершения преступления [7]. В судебной практике нередко возникают ситуации, когда действия виновного лица одновременно содержат признаки нескольких составов преступлений, что требует комплексного анализа всех обстоятельств уголовного дела.

Необходимо учитывать и тот факт, что преступления, связанные с использованием пластиковых карт, постоянно совершенствуются. Преступники

активно используют достижения цифровых технологий, методы анонимизации интернет-трафика, криптовалюту и иные способы сокрытия своей деятельности. В связи с этим криминалистическая методика расследования должна непрерывно адаптироваться к современным условиям развития информационного общества [5].

Снижение уровня подобных преступлений невозможно исключительно за счет деятельности правоохранительных органов. Важное значение приобретает профилактика, направленная на повышение финансовой грамотности населения и информирование граждан о распространенных способах мошенничества. Банковские организации также должны совершенствовать системы защиты информации, внедрять дополнительные механизмы идентификации клиентов и своевременно выявлять подозрительные финансовые операции.

Подводя итог, следует отметить, что расследование хищений денежных средств с использованием пластиковых карт представляет собой одно из наиболее сложных направлений современной криминалистики. Высокая технологичность преступлений, использование дистанционных способов совершения противоправных действий и постоянное изменение преступных схем требуют совершенствования методов выявления и расследования подобных деяний. Повышение эффективности противодействия данным преступлениям возможно только при условии комплексного взаимодействия правоохранительных органов, кредитных организаций и специалистов в области информационных технологий.

Список использованных источников

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 09.04.2026). – [Электронный ресурс]. – Режим доступа: https://www.consultant.ru

2. Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 09.04.2026) «О национальной платежной системе». – [Электронный ресурс]. – Режим доступа: https://www.consultant.ru

3. Безручко, Е. В. Актуальные вопросы расследования хищений денежных средств банка с использованием эквайрингового оборудования / Е. В. Безручко, А. А. Романенко // Юристъ – Правоведъ. – 2023. – № 4 (107). – С. 89-95. – EDN: DDGTHJ

4. Воробьева, А. В. Мошенничество с использованием электронных средств платежа – разграничение со смежными составами / А. В. Воробьева, Н. А. Кудрявцева // Вестник науки. – 2024. – Вып. 4. – № 10 (79). – С. 319-325. – EDN: HXZRHR

5. Городнова, А. А. Развитие информационного общества: учебник и практикум для вузов / А. А. Городнова. – 2-е изд., перераб. и доп. – М.: Издательство Юрайт, 2025. – 294 с.

6. Давыдова, О. Э. Особенности расследования преступлений, связанных с Применением банковских карт и их реквизитов / О. Э. Давыдова // Научное сообщество студентов XXI века: экономика, финансы, управление, цифровизация, психология, дизайн, право: Сборник материалов V Межвузовской студенческой научно- практической конференции, Москва, 22 мая 2024 года. – Москва: Московский экономический институт, 2024. – С. 390-397. – EDN: PYLIIT

7. Князькина, А. К. Новые разъяснения Пленума Верховного Суда РФ о краже и мошенничестве в отношении денежных средств с банковского счета и электронных денежных средств / А. К. Князькина // Юрист. – 2024. – № 03. – С. 62-66. – DOI: 10.18572/1812-3929-2024-3-62-66. – EDN: DVKLMG