МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
КАЗАНСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ

Г.И. Сафина, М.В. Талан

КВАЛИФИКАЦИЯ КРАЖИ, СОВЕРШЕННОЙ С БАНКОВСКОГО СЧЕТА, А РАВНО В ОТНОШЕНИИ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ

Методические рекомендации

Казань – 2025

ББК 67.408.121.1
С21

Одобрено редакционно-издательским советом КЮИ МВД России

Рецензенты:
Р.М. Назмеев (Главное следственное управление
МВД по Республике Татарстан);
кандидат экономических наук **М.Н. Трофимов**
(Рязанский филиал Московского университета МВД России им. В.Я. Кикотя)

Авторский коллектив:
Г.И. Сафина – разделы 1 – 4;
М.В. Талан – введение, заключение.

Сафина Г.И.

С21 Квалификация кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств: методические рекомендации / Г.И. Сафина, М.В. Талан. – Казань: КЮИ МВД России, 2025. – 29 с.

ISBN 978-5-907959-16-3

В методических рекомендациях представлены проблемные вопросы квалификации кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств.

Предназначены для преподавателей, адъюнктов и курсантов (слушателей) образовательных организаций системы МВД России, сотрудников органов внутренних дел Российской Федерации.

ISBN 978-5-907959-16-3

ББК 408.121.1

Содержание

Введение

Процесс внедрения информационно-телекоммуникационных технологий необратимый и несет в себе многочисленные положительные аспекты для развития всех сфер жизни общества. Однако вместе с этим чем больше информационные технологии внедряются в нашу жизнь, тем больше преступники пользуются новыми возможностями для совершения преступлений в данной области.

Настоящие методические рекомендации разработаны для оказания помощи сотрудникам правоохранительных органов в квалификации преступления, предусмотренного пунктом «г» части 3 статьи 158 Уголовного кодекса Российской Федерации (УК РФ) – кража, совершенная с банковского счета, а равно в отношении электронных денежных средств. В связи с увеличением количества безналичных расчетов данный вид преступлений приобретает все большую распространенность и требует от сотрудников правоохранительных органов глубокого понимания специфики совершения таких краж, а также умения правильно квалифицировать действия злоумышленников.

Квалифицирующий признак «с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159^3 УК РФ)» введен Федеральным законом от 23 апреля 2018 года № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации». С введения квалифицирующего признака число совершаемых преступлений находится на стабильно высоком уровне, более того они формируют значительную часть тяжких преступлений против собственности.

Показатель	Год					
	2019	2020	2021	2022	2023	2024
Общее количество краж, совершенных с банковского счета, а равно в отношении электронных денежных средств, зарегистрированных в РФ	93 718	169 525	155 379	112 549	117 642	103 414

Изучение судебно-следственной практики указывает на то, что в настоящее время отсутствует единообразная практика применения нормы, предусмотренной пунктом «г» части 3 статьи 158 УК РФ. Возникают вопросы, связанные с квалификацией кражи с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ), отграничением её от иных форм хищений: общеуголовного мошенничества с использованием информационных технологий (ст. 159 УК РФ), мошенничества с использованием электронных средств платежа (ст. 159^3 УК РФ), а также мошенничества в сфере компьютерной информации, совершенного с банковского счета, а равно в отношении электронных денежных средств (п. «в» ч. 3 ст. 159^6 УК РФ).

Таким образом, разработка методических рекомендаций и предоставление сотрудникам правоохранительных органов необходимой информации для правильной квалификации преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ, имеет высокую актуальность и позволяет повысить эффективность расследования таких преступлений.

Цель исследования заключается в разработке научно-методических рекомендаций по совершенствованию практики применения нормы, предусматривающей ответственность за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ). Достижение указанной цели предполагает решение следующих задач:

1) изучить понятия, используемые при расследовании краж, совершенных с банковского счета, а равно в отношении электронных денежных средств;

2) рассмотреть особенности разграничения кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств со смежными составами;

3) исследовать отдельные вопросы квалификации и сформулировать рекомендации по применению нормы, предусмотренной п. «г» ч. 3 ст. 158 УК РФ.

Методологическую основу исследования составляет всеобщий диалектический метод познания, а также общенаучные и специальные методы научного познания, отражающие взаимосвязь теории и практики: системно-структурный, логический, сравнительно-правовой, формально-юридический.

Практическая значимость результатов работы обуславливается тем, что предлагаемые решения могут быть использованы в практической деятельности сотрудников правоохранительных органов и позволят

выработать единообразную практику применения нормы, предусматривающей ответственность за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств; могут быть использованы в образовательном процессе в рамках изучения дисциплин «Уголовное право», «Особенности квалификации отдельных видов преступлений» и в дальнейших научных исследованиях по данной тематике.

Структура работы обусловлена целью и задачами исследования и состоит из введения, четырех разделов, заключения и списка использованной литературы.

Основные понятия, используемые при расследовании краж с банковского счета, а равно в отношении электронных денежных средств

Cookie-файл – небольшой текстовый файл, который веб-сайт сохраняет на компьютере или мобильном устройстве пользователя при посещении сайта. Куки используются для запоминания информации о пользователе, такой как логин, пароль, настройки языка, предпочтения и т.д. Это позволяет веб-сайту «узнавать» пользователя при повторном посещении и предоставлять ему более персонализированный опыт. При расследовании куки могут помочь установить, какие сайты посещал пользователь, что он искал в интернете, и другую информацию, которая может быть полезна для установления его причастности к преступлению.

IMEI (англ. International Mobile Equipment Identity – международный идентификатор мобильного оборудования) – уникальный 15-значный номер, присваиваемый каждому мобильному устройству (телефону, планшету и т.д.). IMEI используется для идентификации устройства в сети мобильного оператора. Он может быть использован для блокировки украденного или потерянного устройства, а также для отслеживания его местоположения. В расследовании IMEI может помочь установить, какое устройство использовалось для совершения преступления, даже если SIM-карта была заменена.

IP-адрес – уникальный числовой адрес, присваиваемый каждому устройству, подключенному к компьютерной сети, использующей протокол IP (например, к Интернету). IP-адрес позволяет устройствам обмениваться данными друг с другом. IP-адрес может быть статическим (постоянным) или динамическим (изменяющимся). В расследовании IP-адрес может помочь установить местоположение устройства, с которого был осуществлен доступ к банковскому счету или электронному кошельку, а также установить личность владельца этого устройства (через запрос к интернет-провайдеру). Каждому провайдеру выделено определенное количество IP-адресов в конкретном диапазоне.

IP-телефония – это технология, позволяющая использовать IP-сеть для ведения международных и междугородных телефонных разговоров и передачи факсов в режиме реального времени. Сигнал передаётся

через сеть, а используемый при этом номер не является городским или абонентским номером операторов связи. Регистрация на использование услуг IP-телефонии может осуществляться через сеть Интернет. При этом не предоставляются документы, подтверждающие личность пользователя.

SIP-телефония (Session Initiation Protocol Telephony) – технология, позволяющая осуществлять телефонные звонки через Интернет, используя протокол SIP. SIP-телефония предоставляет множество преимуществ по сравнению с традиционной телефонной связью, таких как более низкая стоимость звонков, гибкость и масштабируемость. Отличается от привычной сотовой связи тем, что не требует от стороны наличия сотового аппарата или подключения к базовой станции. В расследовании SIP-телефония может быть использована злоумышленниками для совершения звонков с подменой номера, что затрудняет идентификацию звонящего. Запросы к провайдерам SIP-телефонии могут помочь установить реальный номер звонившего и его местоположение.

VPN (виртуальная частная сеть). Смысл виртуальной частной сети заключается в том, что пользователь перед тем, как выйти в сеть, подключается к серверу третьего лица, как правило, локализующегося на территории другого государства. Цель VPN-технологий состоит в максимальной степени обособления потоков данных одной организации от потоков данных всех других пользователей сети общего пользования. Обособленность должна быть обеспечена в отношении параметров пропускной способности потоков и в конфиденциальности передаваемых данных. Для анонимности в сети лица, совершающие хищения с использованием информационно-коммуникационных технологий (далее – ИКТ), могут использовать программу «Тор браузер».

Web-сайт (англ. – Web site) – информационный источник в сети Интернет. На Web-сайте размещена группа объединенных по смыслу страниц гипертекста, доступ к которой возможен по конкретному адресу.

Web-страница (англ. Web page) – составная часть Web-сайта, страница гипертекста. Может содержать текст, изображение и другие элементы. При просмотре web-страницы на экран компьютера выводится страница либо ее часть, размер страницы может быть различным и зависит от объема и типа размещенной информации.

Абонентский номер – последовательность цифр, присвоенная пользователю или абоненту телефонной сети, зная которую, можно ему позвонить. Он состоит из 11 последовательных цифр, 1-я из них определяет код страны, 2, 3, 4-я определяют принадлежность абонентского

номера к региону или оператору сотовой связи, остальные – определяющий номер клиента. Для установления принадлежности абонентского номера к тому или иному сотовому оператору необходимо получить выписку из ресурса нумерации «Федерального агентства связи», который находится в открытом доступе на сайте www.rossvyaz.ru.

Аккаунт (с английского account; часто используются также следующие термины: профиль, учетная запись, личный кабинет) – запись, содержащая набор сведений о пользователе, зарегистрированном в какой-либо социальной сети или интернет-сайте.

Банковская тайна – информация об операциях, счетах и вкладах клиентов и корреспондентов кредитной организации, а также сведениях о клиентах.

БИН банка (Bank Identification Number) – первые 6 цифр номера банковской карты, которые идентифицируют банк-эмитент карты. БИН банка позволяет определить, какой банк выпустил карту, а также тип карты (Visa, Mastercard и т.д.).

Виртуальный номер – телефонный номер, который не привязан к конкретной SIM-карте или физическому устройству. Виртуальные номера используются для различных целей, таких как защита конфиденциальности, создание нескольких телефонных номеров для бизнеса, или совершение звонков из-за границы. Виртуальные номера бывают 3 видов: номер для приема звонков, номер для приема SMS, номер для приема факса. В расследовании виртуальные номера часто используются злоумышленниками для совершения звонков с подменой номера или для регистрации аккаунтов в социальных сетях и других сервисах. Запросы к провайдерам виртуальных номеров могут помочь установить личность пользователя, зарегистрировавшего виртуальный номер.

Вредоносное программное обеспечение (malware – сокращение от malicious software: **malicious** – злонамеренный и soft**ware** – программное обеспечение) – общепринятый термин, используемый для обозначения любого программного обеспечения, специально созданного для того, чтобы причинять ущерб отдельному компьютеру, серверу, или компьютерной сети. Вредоносные программы представляют собой широкую категорию программного обеспечения. Они устанавливаются без разрешения пользователя и влияют на работу компьютера или сотового телефона, могут использоваться для совершения хищений денежных средств.

Доменное имя – уникальное имя, идентифицирующее веб-сайт в Интернете (например, google.com, wikipedia.org). Доменное имя использу-

ется для облегчения доступа к веб-сайту, так как пользователям легче запомнить доменное имя, чем IP-адрес. В расследовании доменные имена могут использоваться злоумышленниками для создания фишинговых сайтов, имитирующих настоящие веб-сайты банков или других организаций. Запросы к регистраторам доменных имен могут помочь установить владельца доменного имени и его контактные данные.

Дроп – сленговое слово, обозначающее того человека, который соглашается, чтобы его банковская карта стала «транзитной» для похищенных денежных средств. **Дроп** переводит незаконно полученные денежные средства между разными счетами. Такая цепочка переводов нужна для того, чтобы скрыть следы киберпреступников и усложнить работу правоохранительных органов.

Интернет – всемирная открытая информационная компьютерная сеть, не имеющая определенной организационной структуры и объединяющая в единое целое для совместного использования множество обновляемых информационных ресурсов и компьютерных сетей, работающих по единым протоколам. Обеспечивает ряд сервисов: электронную почту, передачу файлов, интерактивные конференции, группы новостей, WWW и др. Это – деловая, образовательная, развлекательная информация, электронные газеты и журналы, базы данных практически по всем областям жизнедеятельности общества, доступ к разнообразным информационным ресурсам библиотек, государственных и частных учреждений и компаний.

Интернет-магазин – веб-сайт, позволяющий пользователям покупать товары или услуги через Интернет. Интернет-магазины предоставляют широкий выбор товаров и услуг, а также удобные способы оплаты и доставки. Запросы в интернет-магазины могут помочь установить, какие товары были куплены с использованием похищенных денежных средств, а также установить личность покупателя.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники **(**Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Мессенджеры – класс программ, предназначенных для обмена сообщениями через сеть в реальном времени (Служба мгновенных сообщений – Instant Messaging Service – IMS). Передаваться могут текстовые сообщения, звуковые сигналы, картинки, видео.

Оператор связи – физическое или юридическое лицо, имеющее право на предоставление услуг электрической или почтовой связи (Федеральный закон от 16 февраля 1995 г. № 15-ФЗ «О связи»).

Платежная карта – это пластиковая карта, на которой записываются идентификационные данные об ее держателе, предназначенная для совершения расчетных платежей.

Платежная система – система, обеспечивающая проведение платежей между покупателями и продавцами, включающая оператора платежной системы, операторов услуг платежной инфраструктуры и участников платежной системы, из которых как минимум три организации являются операторами по переводу денежных средств. Запросы в платежные системы могут помочь установить, какие транзакции были совершены с использованием похищенных денежных средств, а также установить личность получателя денежных средств.

Провайдер (оператор связи, поставщик услуг) – компания, предоставляющая пользователям доступ к Интернету. Провайдеры предоставляют различные услуги, такие как подключение к Интернету, электронная почта, хостинг веб-сайтов и т.д. В расследовании запросы к интернет-провайдерам могут помочь установить личность пользователя, которому был присвоен определенный IP-адрес в определенное время.

Tor браузер – программное обеспечение с открытым исходным кодом для обеспечения анонимной связи. Он направляет интернет-трафик через бесплатную всемирную добровольную оверлейную сеть, состоящую из более чем шести тысяч ретрансляторов, для сокрытия местоположения и использования пользователя от любого, кто проводит сетевое наблюдение или анализ трафика. Использование Tor затрудняет отслеживание интернет-активности пользователя

Фишинг – это такой вид мошенничества, когда злоумышленник вынуждает вас совершить действие, позволяющее ему получить доступ к вашему устройству, учетным записям или персональным данным.

Фишинговый сайт – веб-сайт, внешне похожий на доверенный источник, например страницу популярной компании или платежной системы. Такие сайты создают, чтобы похищать данные пользователей: логины и пароли, переписки, банковские реквизиты, служебную информацию и т. д.

Хостинг – это комбинация программных и аппаратных технологий, позволяющая разместить в сети информацию (сайт, приложение, базу

данных и их составные компоненты), требующую постоянного нахождения в онлайне.

Электронное средство платежа – средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств. К электронным средствам платежа относятся: банковские карты (дебетовые, кредитные, предоплаченные); интернет-банкинг и мобильный банкинг; электронные кошельки (например, Яндекс.Деньги, QIWI, WebMoney) и др.

Электронные платёжные системы – используются для проведения финансовых транзакций на рынке облигаций, валютном рынке, на рынке производных финансовых инструментов и опционов и для передачи средств между финансовыми организациями.

Электронный кошелек – это счет, который пользователи открывают в платежной системе. В отличие от банковского счета, у электронного кошелька нет счета в банке, а все данные и деньги хранятся только в приложении на устройстве или на сайте.

Сведения, необходимые для расследования кражи с банковского счета, а равно в отношении электронных денежных средств

Для получения информации, необходимой для расследования краж с банковского счета, а равно в отношении электронных денежных средств, сотрудники правоохранительных органов направляют запросы в различные организации и учреждения. Цель каждого запроса – получить конкретные данные, которые помогут установить обстоятельства преступления, личность преступника и вернуть похищенные средства. Как правило, запросы направляются в:

Банки и другие кредитные организации

♦ Выписки по счетам потерпевшего и подозреваемых

♦ Информация о транзакциях, включая дату, время, сумму, назначение платежа, реквизиты отправителя и получателя

♦ IP-адреса, с которых осуществлялись операции по счетам

♦ Информация о блокировках счетов и причинах блокировки

♦ Данные о владельцах счетов (ФИО, паспортные данные, адрес регистрации)

♦ Информация о привязке банковских карт к счетам

Платежные системы

♦ Запрашиваемая информация аналогична запросам в банки, но относится к электронным кошелькам и операциям с ними

Операторы сотовой связи

♦ Данные о владельце номера телефона (ФИО, паспортные данные, адрес регистрации)

♦ Детализация звонков и SMS-сообщений (дата, время, номер абонента, продолжительность звонка, текст SMS)

♦ Информация о местоположении абонента в момент совершения звонка или отправки SMS (базовая станция, координаты)

♦ Информация об IMEI (International Mobile Equipment Identity) – уникальном идентификаторе мобильного устройства

Интернет-магазины и сайты объявлений

♦ Информация о заказах, совершенных с использованием определенной банковской карты или электронного кошелька

♦ Данные о покупателе (ФИО, адрес доставки, номер телефона, адрес электронной почты)

♦ IP-адрес, с которого был сделан заказ

Информация о доставке товара (дата, время, адрес доставки, данные курьера)

♦ История переписки с покупателем

♦ Информация о возвратах товара

Интернет-провайдеры

♦ Информация об IP-адресах, с которых осуществлялся доступ к определенным ресурсам в определенное время

♦ Данные о владельце IP-адреса (ФИО, адрес регистрации)

Регистраторы доменных имен

♦ Данные о владельце доменного имени (ФИО, адрес регистрации, контактные данные)

♦ Информация о дате регистрации доменного имени

♦ Информация о сервере, на котором размещен сайт

Социальные сети

♦ Данные о пользователе (ФИО, дата рождения, адрес регистрации, контактные данные)

♦ IP-адреса, с которых осуществлялся доступ к аккаунту

♦ История переписки пользователя

♦ Информация о друзьях и подписчиках пользователя

♦ Фотографии и видеозаписи, размещенные пользователем

♦ Информация о геолокации пользователя.

♦ Информация о группах и сообществах, в которых состоит пользователь

Правоохранительные органы других регионов и стран

♦ Любая информация, необходимая для расследования в рамках международного сотрудничества

Важно отметить, что запросы должны быть обоснованы необходимостью получения информации для расследования конкретного уголовного дела. Сотрудники правоохранительных органов обязаны соблюдать конфиденциальность полученной информации и использовать ее только в целях расследования уголовного дела. Для получения информации, составляющей тайну переписки или иную охраняемую законом тайну, необходимо получение судебного решения (санкции суда).

Полезные сервисы для расследования краж с банковского счета, а равно в отношении электронных денежных средств[1]

♦ Сервис для проверки банковского идентификационного номера (необходимо ввести первые 6 цифр номера платежной карты): https://bincheck.io/index.php/ru

♦ Сервис, который позволяет узнать основные данные о доменном имени (кто администратор и регистратор, срок регистрации и другие данные): https://www.reg.ru/whois/

♦ Сервис для определения IP-адреса сервера, его местоположения и дополнительной информации о сайте (необходимо ввести доменное имя или имя хоста): https://www.ip-tracker.org

♦ Сервис для повышения качества фотографии: https://www.waifu2x.net

♦ Многофункциональный поисковый сервис, который осуществляет поиск в скрытой части интернета, платформы для обмена документами, базы данных whois, утечки общедоступных данных и других местах: https://intelx.io

♦ Сервис определения местоположения (географические координаты и адреса) базовых станций сотовой связи по их параметрам (MCC, MNC, LAC и Cell ID): xinit.ru/bs/

♦ Сервис для определения сотового оператора и региона (или город и страну) по любому номеру телефона в России или в мире: https://www.kody.su/check-tel#text

♦ Сервис для получения информации об IP-адресе или домене: https://2ip.ru/whois/#result-anchor

---

[1] Информация носит справочно-информационный характер и не подтверждает обстоятельств, входящих в предмет доказывания.

Особенности разграничения кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств, с иными смежными составами

В Российской Федерации хищения в отношении безналичных и электронных денежных средств в зависимости от способа совершения квалифицируют по соответствующей части ст. 158 («Кража»), 159 («Мошенничество»), 159^3 («Мошенничество с использованием электронных средств платежа»), 159^6 («Мошенничество в сфере компьютерной информации») УК РФ.

Квалифицирующий признак, указанный в п. «г» ч. 3 ст. 158 УК РФ («с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159^3 УК РФ»)) уже заложил в себе необходимость отграничения его от смежного преступления, предусмотренного ст. 159^3 УК РФ «Мошенничество с использованием электронных средств платежа».

К сожалению, единообразное понимание и применение нормы ст. 159^3 УК РФ до сих пор отсутствует, вследствие чего дела по рассматриваемой норме практически не возбуждаются. Согласно толкованию понятия мошенничества, изъятие безналичных денежных средств должно осуществляться путем обмана или злоупотребления доверием,

при этом средством совершения преступления должно быть электронное средство платежа.

На наш взгляд, по ст. 159[3] УК РФ следует квалифицировать деяния, когда владелец банковского счета под воздействием обмана и (или) злоупотребления доверием (под предлогом блокировки, взлома счёта; оформления кредита; дополнительного заработка и т.д.) перечисляет денежные средства на счет (банковский, абонентского номера, электронный кошелек и т.д.) преступника через мобильный банк, банкомат, систему денежных переводов и т.п. В настоящее время в судебно-следственной практике подобные факты квалифицируются по общей норме, предусмотренной ст. 159 УК РФ.

При квалификации деяния как «Мошенничество» (ст. 159 УК РФ) основное отличие заключается в способе совершения преступления. При краже происходит тайное хищение денежных средств без ведома владельца. При мошенничестве владелец сам передает денежные средства злоумышленнику под воздействием обмана или злоупотребления доверием. Например, если потерпевший сам перевел деньги на счет мошенника, поверив в ложное сообщение о выигрыше в лотерею, о блокировке счета, о том, что родственник попал в беду, это будет квалифицировано как мошенничество.

Ст. 159[6] УК РФ «Мошенничество в сфере компьютерной информации», согласно пояснительной записке, связана с хищением или приобретением права на чужое имущество, сопряженное с преодолением компьютерной защиты имущества (имущественных прав). Подобные преступления совершаются не путем обмана или злоупотребления доверием конкретного субъекта, а путем получения доступа к компьютерной системе и совершения вышеуказанных действий, которые в результате приводят к хищению чужого имущества или приобретению права на чужое имущество[1].

Воздействие на технические устройства или сети должно происходить путем воздействия программных и (или) программно-аппаратных средств. В описанном способе обман, привычный для мошенничества, отсутствует.

Исходя из изложенного, состав, предусмотренный ст. 159[6] УК РФ, мошенничеством по своей сути не является, а представляет собой лишь

---

[1] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации (в части дифференциации мошенничества на отдельные составы): пояснительная записка. URL: https://sozd.duma.gov.ru/bill/53700-6 (дата обращения: 06.06.2024).

форму хищения с использованием специфических средств, которые обозначены в диспозиции статьи, так как обмануть или злоупотребить доверием компьютерной техники невозможно[1].

В настоящее время, исходя из анализа судебной практики, приходим к выводу, что как мошенничество в сфере компьютерной информации квалифицируют деяния, когда лицо, обладающее специальными познаниями в сфере информационных технологий, разрабатывает, использует программные обеспечения, приложения, позволяющие разрушать защиту информационных систем, получать доступ к компьютерной информации. Как справедливо отмечает С.В. Шевелева, это сложное преступление, состоящее из других преступлений-способов[2].

Главным критерием отграничения преступления, предусмотренного п. «в» ч. 3 ст. 159^6 УК РФ, является способ совершения преступления. При совершении мошенничества в сфере компьютерной информации происходит вмешательство в работу компьютерных систем или сетей. При краже, предусмотренной п. «г» ч. 3 ст. 158 УК РФ, доступ к банковскому счету или электронному кошельку осуществляется с помощью легальных средств авторизации.

При мошенничестве также предметом преступления, помимо имущества, могут выступать имущественные права.

Гр. П., обладая информацией о наличии у ООО «РОМИР Панель» электронных подарочных сертификатов интернет-магазинов «Озон», «Вайлдберриз», представляющих собой коды доступа в виде набора буквенных и числовых обозначений, позволяющих в дистанционном режиме производить оплату приобретаемых товаров и услуг, путем подбора кодов доступа и их внесения в доменное имя веб-сайта самостоятельно активировал вышеуказанные сертификаты в своем личном кабинете путем пополнения баланса личного кабинета на веб-сайтах интернет-магазинов

[1] Лаврушкина А.А. Проблемы применения ст. 159. 6 УК РФ с позиции теории и практики // Контентус. 2018. № 3 (68). URL: https://cyberleninka.ru/article/n/problemy-primeneniya-stati-159-6-uk-rf-s-pozitsii-teorii-i-praktiki (дата обращения: 15.11.2023).

[2] Шевелева С.В. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами преступлений // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. № 4 (40). URL: https://cyberleninka.ru/article/n/moshennichestvo-v-sfere-kompyuternoy-informatsii-osobennosti-kvalifikatsii-i-konkurentsii-so-smezhnymi-sostavami-prestupleniy (дата обращения: 11.12.2023).

«Озон», «Вайлдберриз», а также операторов сотовой связи «Билайн», «МТС», «Йота», «Мегафон», «Теле-2» на номинальную стоимость сертификатов. Тем самым получил возможность распоряжаться кодами доступа, принадлежащим ООО «РОМИР Панель» и сертификатам по своему усмотрению, а также реализовывал похищенные коды доступа посредством продажи неустановленным лицам. Гр. П. был осужден по п. «б» ч. 3 ст. 159[6] и ч. 2 ст. 273 УК РФ.

Предметом преступления в рассматриваемом случае стали электронные подарочные сертификаты. Определения подарочных сертификатов в законодательстве не содержится. Согласно Письму Минфина от 25 апреля 2011 г. № 03-03-06/1/268, в качестве подарочного сертификата принято понимать документ, удостоверяющий право его держателя приобрести у лица, выпустившего сертификат, товары, работы или услуги на сумму, равную номинальной стоимости этого сертификата[1]. Подарочный сертификат представляет собой имущественное право; соответственно деяние было квалифицировано как мошенничество.

Для правильной квалификации хищения безналичных денежных средств по соответствующей норме УК РФ следует:

Установить факт хищения

Необходимо установить, что денежные средства были списаны с банковского счета или электронного кошелька без согласия владельца

Установить способ хищения

Необходимо установить, каким образом был осуществлен доступ к счету или ЭДС. Это может быть фишинг, скимминг, использование вредоносного программного обеспечения, социальная инженерия и т.д.

Установить сумму ущерба и определить квалифицирующие признаки

- Необходимо определить не имеет ли место малозначительное деяние
- Необходимо определить, какие имеются квалифицирующие признаки (например, совершение группой лиц по предварительному сговору, в крупном размере и т.д.)

[1] Письмо Департамента налоговой и таможенно-тарифной политики Минфина РФ от 25.04.2011 № 03-03-06/1/268. URL: https://www.garant.ru/products/ipo/prime/doc/12085421/ (дата обращения: 06.06.2024).

Рекомендации по квалификации кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств

Уголовно-правовая характеристика кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств

Объект	Право собственности на денежные средства, находящиеся на банковском счете или электронном кошельке
Предмет	Денежные средства, находящиеся на банковском счете или электронном кошельке
Объективная сторона	Характеризуется тайным хищением денежных средств с банковского счета или электронного кошелька с причинением имущественного ущерба собственнику
Субъективная сторона	Характеризуется прямым умыслом и корыстной целью на хищение денежных средств. Необходимо установить, что лицо осознавало, что совершает хищение денежных средств с банковского счета или электронного кошелька, и желало этого
Субъект	Физическое вменяемое лицо, достигшее 14-летнего возраста

1. Одним из распространенных способов кражи с банковского счета является – использование платежной карты. Действия лица, обнаружившего потерянную платежную карту, не предпринявшего никаких действий, направленных на возвращение данной платежной карты ее владельцу или в банк-эмитент, либо в правоохранительные органы, либо похитившего платежную карту и совершившего изъятие денежных средств с банковского счета (расплатилось в магазине, сняло наличные денежные средства в банкомате), подлежат квалификации по п. «г» ч. 3 ст. 158 УК РФ[1].

[1] Киктенко А.А. Уголовная ответственность за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств: автореф. дис. ... канд. юрид. наук. Москва, 2023. С 9.

Чаще данный вид кражи совершается с неопределенным умыслом, когда виновное лицо не знает, какая сумма денежных средств находится на счёте. Традиционно в уголовном праве деяние с неопределенным умыслом предлагается квалифицировать по фактически наступившим общественно опасным последствиям.

Часто виновные оплачивают покупки в разных магазинах на сумму, для которой не требуется введения пин-кода в терминале оплаты, пока не истратят все средства на счете платежной карты либо ее не заблокируют. При оплате нескольких покупок с использованием чужой банковской карты в разных организациях данное преступление следует считать единым продолжаемым преступлением.

В Постановлении Пленума Верховного Суда РФ от 12.12.2023 № 43 «О некоторых вопросах судебной практики по уголовным делам о длящихся и продолжаемых преступлениях» указывается, что о единстве умысла виновного в указанных случаях могут свидетельствовать, в частности, такие обстоятельства, как совершение тождественных деяний с незначительным разрывом во времени, аналогичным способом, в отношении одного и того же объекта преступного посягательства и (или) предмета преступления, направленность деяний на достижение общей цели.

Когда хищение денежных средств осуществляется путем систематического противоправного использования чужой банковской карты, деяние считается продолжаемым преступлением с единым умыслом распорядиться денежными средствами на счёте.

2. Распространенным примером хищения денежных средств с банковского счета являются случаи, когда виновный похищает иное имущество (сотовый телефон, кошелек и др.), впоследствии с помощью которого совершает кражу с банковского счета, а равно в отношении электронных денежных средств, предусмотренную п. «г» ч. 3 ст. 158 УК РФ. Следственно-судебная практика указанные преступные действия квалифицирует по-разному: как единое продолжаемое преступление, где кража иного имущества является способом совершения более тяжкого преступления; либо как совокупность кражи и кражи, предусмотренной п. «г» ч. 3 ст. 158 УК РФ.

Московский районный суд города Санкт-Петербурга осудил гр. Х. по п. «г» ч. 3 ст. 158 УК РФ за совершение преступления при следующих обстоятельствах: гр. Х. путем свободного доступа завладел сотовым телефоном «Редми 8Т»

с находящейся внутри сим-картой, после чего переставил указанную выше сим-карту в находившийся при нем сотовый телефон «Нокиа», тем самым получил доступ к счёту банковской карты, привязанного к абонентскому номеру потерпевшего. Реализуя свой преступный умысел, направленный на тайное хищение денежных средств, гр. Х. воспользовавшись услугой банка СМС-банкинга, отправил сообщение (СМС-команду) и совершил перевод денежных средств на сумму 7 900 рублей на банковский счёт гр. А., неосведомленного о преступных действиях гр. Х. Похищенный ранее сотовый телефон продал в скупку[1].

В вышеуказанном примере суд квалифицировал действия гр. Х. только по п. «г» ч. 3 ст. 158 УК РФ, указав, что полностью доказан квалифицирующий признак совершения подсудимым тайного хищения чужого имущества и с банковского счета. Однако в описательной части приговора указывается ущерб в сумме 7900 рублей без учета стоимости сотового телефона.

Согласно постановлению Пленума Верховного Суда Российской Федерации от 27 декабря 2002 года № 29 «О судебной практике по делам о краже, грабеже и разбое», в случае совершения кражи при отягчающих обстоятельствах действия виновного при отсутствии реальной совокупности преступлений подлежат квалификации лишь по той части указанных статей УК РФ, по которой предусмотрено более строгое наказание. При этом в описательной части приговора должны быть приведены все квалифицирующие признаки деяния.

По нашему мнению, при краже иного имущества с последующей кражей безналичных денежных средств деяние необходимо квалифицировать исходя из направленности умысла виновного, подтверждённого объективными данными. Однако кража иного имущества в любом случае не должна оставаться без уголовно-правовой оценки. Если кража иного имущества была способом совершения более тяжкого преступления, необходимо квалифицировать по той части статьи, которая предусматривает более строгое наказание, с указанием квалифицирующих признаков в описательной части приговора суда. Если же умысел виновного изначально был направлен на кражу иного имущества, а затем он обнаружил возможность кражи безналичных денежных средств, то такое преступление подлежит квалификации как совокупность преступлений.

[1] Приговор Московского районного суда г. Санкт-Петербурга от 27.10.2022 по делу № 1-901/22. URL: https://msk spb.sudrf.ru (дата обращения: 12.06.2024).

3. Встречаются случаи насильственного хищения безналичных денежных средств.

Гр. А. совершил разбой при следующих обстоятельствах: находясь на улице подошел к ранее незнакомому гр. Б. и задал последнему вопрос – есть ли у того денежные средства, получив отрицательный ответ, гр. А. с целью реализации задуманного, а также подавления воли гр. Б. к сопротивлению, достал из кармана нож и продемонстрировал его, сказав при этом, что у него имеется нож и если последний убежит, то он его догонит. Далее гр. А. потребовал от гр. Б. показать, сколько у него денежных средств на расчетном счете в мобильном банке, что гр. Б. и сделал. Увидев наличие денежных средств на счете, гр. А., потребовал от гр. Б. перевести ему денежные средства. После этого гр. А. с места совершения преступления скрылся, распорядившись похищенными денежными средствами по своему усмотрению. Действия гр. А. квалифицированы по ч. 2 ст. 162 УК РФ[1].

Учитывая, что законом не предусмотрен квалифицирующий признак совершения грабежа или разбоя с банковского счета, а равно в отношении электронных денежных средств, содеянное в таких случаях следует квалифицировать (при отсутствии других квалифицирующих признаков, указанных в диспозициях соответствующих статей УК РФ) по ч. 1 ст. 161 либо ч. 1 ст. 162 УК РФ. Последующее списание безналичных денежных средств со счета платежной карты является актом распоряжения виновного похищенным имуществом и не образует совокупности с составом, предусмотренным п. «г» ч. 3 ст. 158 УК РФ. Однако, если преступный умысел у виновного возник после совершения грабежа или разбоя, данные действия рекомендуется квалифицировать как совокупность преступлений, предусмотренных соответствующей частью ст. 161 или ст. 162 и п. «г» ч. 3 ст. 158 УК РФ.

[1] Приговор Басманного районного суда г. Москвы от 01.11.2021 по делу № 1-373/21. URL: https://mos-gorsud.ru/ (дата обращения: 22.04.2024).

Заключение

Квалификация кражи с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ) требует от сотрудников правоохранительных органов глубокого понимания специфики совершения таких преступлений, а также умения правильно разграничивать их со смежными составами преступлений. Настоящие методические рекомендации призваны помочь сотрудникам правоохранительных органов в решении этих задач.

Важно помнить, что развитие информационных технологий постоянно порождает новые способы совершения преступлений в сфере безналичных расчетов. Поэтому сотрудникам правоохранительных органов необходимо постоянно повышать свою квалификацию, изучать новые методы и технологии, используемые злоумышленниками.

Проведенное исследование позволило предложить ряд рекомендаций по квалификации кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств:

♦ критерием отграничения преступлений, предусмотренных п. «г» ч. 3 ст. 158 УК РФ и ст. 159^3 УК РФ, является способ хищения: кража, совершенная с банковского счета, а равно в отношении электронных денежных средств, совершается тайно, а мошенничество предполагает обман или злоупотребление доверием. При тайном хищении денежных средств оно совершается без ведома и согласия собственника имущества. Владелец счета или электронных денежных средств не осознает, что у него похищают безналичные денежные средства и не участвует в передаче средств. Например, несанкционированный доступ к банковскому счету или электронным денежным средствам (взлом, использование вредоносного ПО, скимминг, фишинг с последующим несанкционированным переводом безналичных денежных средств);

♦ критерием отграничения преступлений, предусмотренных п. «г» ч. 3 ст. 158 УК РФ и п. «в» ч. 3 ст. 159^6 УК РФ, является способ совершения преступления: в одном случае доступ к банковскому счету или электронному кошельку осуществляется с помощью легальных средств авторизации, а в другом – путем воздействия программных и (или) программно-аппаратных средств на серверы и средства вычислительной техники;

♦ если платежная карта неправомерно использовалась для оплаты товаров или услуг в торговой точке, для онлайн-платежей или перевода денежных средств, деяние квалифицируется как кража;

♦ при оплате нескольких покупок с использованием чужой платежной карты в разных организациях, охватываемых единым преступным умыслом, данное преступление следует считать единым продолжаемым преступлением;

♦ при краже иного имущества с последующей кражей безналичных денежных средств деяние необходимо квалифицировать исходя из направленности умысла виновного, подтверждённого объективными данными. Однако кража иного имущества в любом случае не должна оставаться без уголовно-правовой оценки. Если кража иного имущества была способом облегчения совершения кражи с банковского счета, а равно в отношении электронных денежных средств, то следует квалифицировать только по п. «г» ч. 3 ст. 158 УК РФ. Если же умысел виновного изначально был направлен на кражу иного имущества, а затем он обнаружил возможность кражи безналичных денежных средств, то такое преступление подлежит квалификации как совокупность преступлений;

♦ открытое или насильственное умышленное хищение безналичных денежных средств не образует совокупности с п. «г» ч. 3 ст. 158 УК РФ, квалификация должна быть по соответствующей части ст. 161 или ст. 162 УК РФ.

Список использованной литературы

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 14.03.2020 № 1-ФКЗ, и изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Российская газета. – 1993. – 25 декабря.

2. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 08.08.2024) // Собрание законодательства Российской Федерации. – 1996. – № 25, ст. 2954.

3. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 № 174-ФЗ (ред. от 01.07.2024) // Собрание законодательства Российской Федерации. – 2001. – № 52 (ч. I), ст. 4921.

4. О национальной платежной системе: Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 19.12.2023) // Собрание законодательства Российской Федерации. – 2011. – № 27, ст. 3872.

5. О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 23.04.2018 № 111-ФЗ // Российская газета. – 2018. – № 88.

6. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации (в части дифференциации мошенничества на отдельные составы): пояснительная записка. URL: https://sozd.duma.gov.ru/bill/53700-6 (дата обращения: 06.06.2024).

7. О судебной практике по делам о краже, грабеже и разбое: от 27.12.2002 № 29 (ред. от 15.12.2022) // Бюллетень Верховного Суда Российской Федерации. – 2003. – № 2.

8. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 (ред. от 15.12.2022) // Бюллетень Верховного Суда Российской Федерации. – 2018. – № 2.

9. О некоторых вопросах судебной практики по уголовным делам о длящихся и продолжаемых преступлениях: постановление Пленума Верховного Суда Российской Федерации от 12.12.2023 № 43. URL: https://www.vsrf.ru/documents/own/33243/ (дата обращения: 06.06.2024).

10. Письмо Департамента налоговой и таможенно-тарифной политики Минфина Российской Федерации от 25.04.2011 № 03-03-06/1/268. URL: https://www.garant.ru/products/ipo/prime/doc/12085421/ (дата обращения: 06.05.2024).

II. Научные статьи

1. Шевелева С.В. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами преступлений // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2017. – № 4 (40). URL: https://cyberleninka.ru/article/n/moshennichestvo-v-sfere-kompyuternoy-informatsii-osobennosti-kvalifikatsii-i-konkurentsii-so-smezhnymi-sostavami-prestupleniy (дата обращения: 11.12.2023).

2. Лаврушкина А.А. Проблемы применения ст. 159^6 УК РФ с позиции теории и практики // Контентус. – 2018. – № 3 (68). URL: https://cyberleninka.ru/article/n/problemy-primeneniya-stati-159-6-uk-rf-s-pozitsii-teorii-i-praktiki (дата обращения: 15.11.2023).

III. Материалы судебной практики

1. Приговор Басманного районного суда г. Москвы от 01.11.2021 по делу № 1-373/21. URL: https://mos-gorsud.ru/ (дата обращения: 22.04.2022).

2. Приговор Московского районного суда г. Санкт-Петербурга от 27.10.2022 по делу № 1-901/22. URL: https://msk.spb.sudrf.ru (дата обращения: 12.06.2022).

IV. Диссертации, авторефераты диссертаций

1. Киктенко А.А. Уголовная ответственность за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств: дис. ... канд. юрид. наук: 5.1.4 / Киктенко Анна Александровна. – Москва, 2023. – 162 с.

2. Шавалеев Б.Э. Мошенничество с использованием электронных средств платежа: уголовно-правовой и криминологический аспекты: автореф. дис. ... канд. юрид. наук. – Казань, 2024. – 30 с.

V. Публикации в средствах массовой информации

Статистические сведения о преступлениях за 2013 – 2024 гг. // ФКУ «ГИАЦ МВД России». URL: https://xn--b1aew.xn--p1ai/folder/101762 (дата обращения: 12.02.2024).

Учебное издание

Сафина Гульнара Ильгизовна
Талан Мария Вячеславовна

КВАЛИФИКАЦИЯ КРАЖИ, СОВЕРШЕННОЙ С БАНКОВСКОГО СЧЕТА, А РАВНО В ОТНОШЕНИИ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ

Методические рекомендации

Корректура, компьютерная верстка,
дизайн обложки О.В. Добрыдневой

Формат 60*84 1/16
Усл. печ. л. 2
Дата подписания в печать 20.04.2025
Тираж 40 экз.

Типография КЮИ МВД России
420064, г. Казань, ул. Оренбургский тракт, 130