



УДК 343.9



Елена Алексеевна ХАРИНА,

доцент кафедры криминалистики
Сибирского юридического института
МВД России (г. Красноярск),
кандидат юридических наук
elna.harina@yandex.ru

ТИПИЧНЫЕ СПОСОБЫ КРАЖ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

TYPICAL WAYS OF COMMITTING THEFTS USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

В статье на основе анализа статистических данных о зарегистрированных и раскрытых хищениях, совершенных с использованием информационно-телекоммуникационных технологий (ИТТ), аргументируется вывод о неоднородной судебной-следственной практике применения уголовно-правовых норм, предусматривающих уголовную ответственность за совершение краж, совершенных с использованием ИТТ, приводится авторская классификация типичных способов анализируемого деяния, рассматриваются типичные ошибки, допускаемые правоприменителями при квалификации деяний.

The article, based on an analysis of statistical data on registered and solved thefts committed using information and telecommunication technologies (ITT), substantiates the conclusion that the judicial and investigative practice of applying criminal legal norms providing for criminal liability for thefts committed with the use of ITT is heterogeneous. The author's classification of typical ways of the offence in question is presented, and typical mistakes made by law enforcement officials in qualifying these acts are considered.

Ключевые слова: хищения, совершенные с использованием информационно-телекоммуникационных технологий, типичные способы краж, информационно-телекоммуникационные технологии.

Keywords: theft committed using information and telecommunication technologies, typical ways of thefts, information and telecommunication technologies.

Современное состояние преступности указывает на наличие тенденции систематического роста количества преступлений, совершенных с использованием информационно-телекоммуникационных технологий (далее – ИТТ). Этот процесс естественен и является следствием развития научно-технологического прогресса.

Наряду с этим необходимо отметить, что в 2025 г. впервые отмечено снижение количества зарегистрированных преступлений рассматриваемой категории. Так, согласно официальным данным МВД России¹ в 2025 г. в Российской Федерации зарегистрированы 675 372 преступления, совершенных с использованием ИТТ, что на 11,8% меньше

¹ Официальный сайт МВД России. URL: <https://мвд.рф/reports/item/77848182/> (дата обращения: 10.02.2026).



по сравнению с показателями прошлого года. В целом же доля исследуемых преступных деяний относительно общего количества всех зарегистрированных преступлений уменьшилась на 1,9% и составляет 38,1%¹. Отрицательная динамика вселяет оптимизм и является результатом государственно-правового реагирования и противодействия возникающим угрозам.

Одну из лидирующих позиций среди зарегистрированных хищений, совершенных с использованием ИТТ, в 2025 г. занимают кражи (80 956 преступлений). Несмотря на то, что в целом раскрываемость рассматриваемой категории краж (36%) выше среднего процента раскрываемости всех преступлений, совершенных с использованием ИТТ (26,6%)², имеющийся уровень противодействия трудно назвать эффективным, что свидетельствует о необходимости уделения данному вопросу более пристального внимания.

Анализ судебной-следственной практики позволил прийти к выводу о наличии неоднородной практики применения норм, предусматривающих ответственность за совершение хищений с использованием ИТТ, что связано с имеющимися проблемами квалификации деяний, в частности их отграничения от смежных составов. В этой связи считаем целесообразным осветить некоторые проблемные вопросы, с которыми сталкиваются правоприменители в процессе квалификации преступных деяний.

Как известно, преимущественное большинство краж, совершенных с использованием ИТТ, квалифицируются по п. «г» ч. 3 ст. 158 УК РФ как кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ). Изучение судебной-следственной практики показало, что с наибольшими трудностями правоприменители сталкиваются при отграничении указан-

ного квалифицированного состава кражи от ст. 159.3 УК РФ (мошенничество с использованием электронных средств платежа) [5; 8].

Так, одним из возникающих вопросов является квалификация деяния при использовании в ходе совершения преступления банкомата для снятия наличных денежных средств. Большинство изученных приговоров свидетельствуют о правильности квалификации деяния по п. «г» ч. 3 ст. 158 УК РФ. Однако имеются случаи иной правовой позиции: переквалификации деяний на п. «в» ч. 2 ст. 158 УК РФ³, а также квалификации таких деяний по ст. 159.3 УК РФ. Стоит отметить, что, несмотря на использование при совершении преступления электронных средств платежа, определяющим фактором при квалификации деяния должно являться наличие или отсутствие в способе совершения хищения обмана или злоупотребления доверием [4, с. 48]. В такой ситуации деяние может являться мошенничеством в случае участия в выдаче денежных средств работника кредитной организации, обманутого или введенного в заблуждение относительно принадлежности банковской карты. Данное положение нашло отражение в п. 25.1 постановления Пленума Верховного Суда РФ от 27 декабря 2002 г. N 29 «О судебной практике по делам о краже, грабеже и разбое», согласно которому снятие наличных денежных средств через банкомат с использованием чужой или поддельной платежной карты надлежит квалифицировать как кражу по признаку «с банковского счета, а равно в отношении электронных денежных средств».

Еще одним выявленным проблемным вопросом является ошибочная квалификация хищений, совершенных посредством оплаты товаров чужой банковской картой, по ст. 159.3 УК РФ [7]. Так, А., похитив кредитную банковскую карту, более пятидесяти раз осуществил оплату приобретенных товаров на общую сумму более 27 тыс.

1 Официальный сайт МВД России. URL: <https://мвд.рф/reports/item/77848182/> (дата обращения: 10.02.2026).

2 Там же.

3 Апелляционное определение Красноярского краевого суда от 18.12.2018 N 22-7584/2018. URL: <https://actofact.ru/case-24OS0000-22-7584-2018-2018-11-21-2-1/> (дата обращения: 07.12.2025).



руб., в результате чего был осужден по ч. 2 ст. 159.3 УК РФ¹. Следует отметить, что такого рода хищения следует квалифицировать по п. «г» ч. 3 ст. 158 УК РФ. Соответствующие разъяснения также даны в п. 25.1 вышеуказанного постановления Пленума Верховного Суда РФ.

Отдельного внимания также требуют ситуации ошибочной квалификации краж, совершенных с использованием учетных данных собственника, по ст. 159.6 УК РФ [подр.: 6], ст. 159 УК РФ². Необходимо отметить, что в данном случае необходимо руководствоваться п. 21 постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. N 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», согласно которому в случаях, «когда хищение совершается 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».

Переходя к рассмотрению типичных способов анализируемой преступной деятельности, отметим, что способ преступления является системообразующим элементом криминалистической характеристики преступления. Не преувеличивая его значимости, А.С. Князьков указывал, что «способ является своеобразным «путем пересечения» связей между элементами криминалистической характеристики умышленных преступлений, поскольку именно в нем проявляется суть преступления как противоправного действия» [3, с. 52]. Действительно, именно уяснение указанной автором «сути преступления» в значительной мере способствует процессу его расследования, а также позволяет в должной

мере определить степень уголовно-правового реагирования на совершенное деяние.

Необходимо отметить, что изучение научной литературы по заявленной тематике указало на отсутствие до настоящего времени систематизированных сведений о типичных способах исследуемой преступной деятельности. В этой связи с учетом выявленных неточностей в правовой оценке деяний на основе изученной судебно-следственной практики выделим наиболее типичные способы краж, совершенных с использованием ИТТ, представленные в авторской классификации, – это деяния, совершенные:

1) посредством использования платежных, банковских карт. Преступления данной категории могут совершаться как с использованием поддельных карт, так и с использованием оригинальных чужих карт, при этом способ получения их в распоряжение может быть различным: украденные, найденные, полученные от потерпевшего. Варианты использования карт, в свою очередь, в зависимости от обладания информацией о пин-коде подразделяются на следующие виды:

– с использованием пин-кода (который известен преступнику заранее или был им подобран). Хищения в таком случае совершаются:

а) путем снятия, перевода денежных средств с использованием банкомата. Так, Д., в силу сложившихся дружеских и доверительных отношений передал Х. свою банковскую карту, а также сообщил пин-код для снятия денежных средств в размере 2000 руб. Однако Х., имея корыстный преступный умысел на тайное хищение чужого имущества, произвел снятие денежных средств в банкоматах на общую сумму более 22 тыс руб., в результате чего приговором суда осужден по п. «г» ч. 3 ст. 158 УК РФ³;

б) путем оплаты товаров, работ, услуг на сумму, требующую введения пин-кода. Так, Н. после смерти сестры обнаружила и

1 Приговор Междуреченского городского суда Кемеровской области от 27.05.2020 по делу N 1-144/2020. URL: <https://sudact.ru/regular/doc/qu4IQPKu1INN/> (дата обращения: 07.12.2025).

2 Приговор Братского городского суда Иркутской области от 19.12.2016 N 1-558/2016. URL: <https://sudact.ru/regular/doc/g09gU4WUC15J/> (дата обращения: 10.09.2025).

3 Приговор Железнодорожного районного суда г. Рязани от 03.03.2025 по делу N 1-40/2025. URL: <https://clck.ru/3PHBtw> (дата обращения: 18.09.2025).



присвоила принадлежавшую последней банковскую карту ПАО «Сбербанк». Пин-код от карты Н. был известен, так как ранее она неоднократно по просьбе сестры приобретала продукты питания и лекарства. Реализуя преступный умысел, Н. систематически в течение двух лет использовала присвоенную карту для оплаты товаров, приобретения билетов, всего на общую сумму более 475 тыс. руб. Приговором суда Н. осуждена по п.п. «в», «г» ч. 3 ст. 158 УК РФ¹;

– без использования пин-кода путем оплаты товаров, работ, услуг на сумму, не требующую введения пин-кода. Так, А. обнаружила на земле утерянную банковскую карту, выданную на имя гр. Б. Обнаружив, что карта оснащена системой бесконтактного платежа, позволяющей производить покупки на сумму до 1000 рублей без введения пин-кода, проследовала в магазины, где в общей сложности произвела восемь покупок. Приговором суда А. осуждена по п. «г» ч. 3 ст. 158 УК РФ²;

2) посредством использования конфиденциальной информации, необходимой для совершения доступа к безналичным денежным средствам. Такого рода информацией могут быть персональные данные владельца, данные платежной, банковской карты, контрольная информация, пароли³. При этом способы получения такой информации могут быть различны:

– посредством использования вредоносных компьютерных программ. Работа таких программ может быть организована на компьютерном устройстве потерпевшего, пользующегося услугами электронной платежной системы [1, с. 11];

– посредством использования доверительных отношений с потерпевшим, свободного доступа к реквизитам платежных карт. Так, Г., достоверно зная о возможности

совершения покупок и оплаты услуг путем введения реквизитов банковской карты без подтверждения операций пин-кодом, фотографировал на свой сотовый телефон с обеих сторон банковские карты, принадлежащие его родственникам. С целью реализации преступного умысла, направленного на хищение денежных средств, фигурант с использованием реквизитов банковских карт неоднократно совершал покупки в приложении «Joom», а также оплачивал услуги интернет-провайдеров, всего на общую сумму более 400 тыс. руб. Приговором суда Г. осужден по п. «г» ч. 3 ст. 158 УК РФ⁴;

– посредством обмана или злоупотребления доверием потерпевшего; использования методов социальной инженерии, фишинговых сайтов и т.п. Так, Ф. на сайте «Авито» подобрал объявления о продаже мебели, стенки и стола, осуществил звонки на указанные в объявлении номера и под предлогом перевода денежных средств в качестве оплаты товара убедил потерпевших сообщить ему конфиденциальную информацию о принадлежащих им банковских картах ПАО «Сбербанк»: номера, срок действия, полученные посредством смс коды безопасности и пароли. Используя полученную информацию, фигурант осуществил несколько переводов денежных средств со счетов потерпевших на принадлежащий ему банковский счет. Приговором суда фигурант осужден по п. «г» ч. 3 ст. 158 УК РФ⁵.

Кроме того, доступ к конфиденциальной информации может быть получен в результате утечек, произошедших в силу неправомерного доступа к различного рода базам данных, а также из чеков, оставляемых у банкоматов после активации услуги онлайн-банкинга [2, с. 30-32].

1 Приговор Дзержинского районного суда г. Перми от 10.03.2025 по делу N 1-82/2025. URL: <https://sudact.ru/regular/doc/WLaOpYVMVmn/> (дата обращения: 27.11.2025).

2 Приговор Альметьевского городского суда Республики Татарстан от 26.03.2025 по делу N 1-142/2025. URL: <https://sudact.ru/regular/doc/jJuae8KD8RLQ/> (дата обращения: 18.09.2025).

3 О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда РФ от 30.11.2017 N 48.

4 Приговор Байkitского районного суда Красноярского края от 25.04.2025 по делу N 1-8/2025. URL: <https://sudact.ru/regular/doc/gW5kiz8jti51/> (дата обращения: 07.12.2025).

5 Приговор Новочебоксарского городского суда Чувашской Республики от 27.07.2020 по делу N 1-283/2020. URL: <https://sudact.ru/regular/doc/jfnFn4DGa6ZJ/> (дата обращения: 07.12.2025).



3) посредством использования абонентского номера потерпевшего, подключенного к услуге «Мобильный банк». Способы получения доступа к управлению денежными средствами могут быть различными.

– получение доступа к телефонному аппарату, подключенному к услуге «Мобильный банк». Способ получения такого доступа может быть различным: потеря или похищение телефонного аппарата, передача потерпевшим во временное пользование. Так, Г. под угрозой насилия, не опасного для жизни и здоровья, совершил хищение сотового телефона марки «Apple iPhone Xr 64GB», а также денежных средств в сумме 1500 руб. После чего достоверно зная, что на телефоне установлено мобильное приложение банка «Тинькофф», а также располагая сведениями о пароле от входа в приложение, совершил перевод денежных средств на сумму более 10 тыс. руб. Приговором суда фигурант осужден по п. «г» ч. 2 ст. 161, п. «г» ч. 3 ст. 158 УК РФ¹;

– приобретение сим-карты, которая бывшим владельцем была подключена (и не отключена) к услуге дистанционного банковского обслуживания. В таком случае у нового владельца сим-карты сохраняется возможность совершать операции с денежными средствами на счетах предыдущего владельца сим-карты. Так, Т., имея умысел на тайное хищение денежных средств, приобрел сим-карту оператора сотовой связи «МТС», активировал ее, присвоив абонентский номер, который ранее использовал потерпевший и к которому была подключена услуга смс-уведомления по кредитной карте, привязанной к расчетному счету в АО «Т Банк». Осуществив доступ в личный кабинет потерпевшего Т. осуществил переводы денежных средств на общую сумму 30 тыс. руб. на бан-

ковский счет, находящийся в его пользовании. Приговором суда Т. осужден по п. «г» ч. 3 ст. 158 УК РФ²;

– использование своего служебного положения сотрудниками организаций, оказывающих услуги связи, а также путем предъявления подложной доверенности на получение дубликата сим-карты;

4) посредством использования своего служебного положения для получения доступа к управлению денежными средствами на счетах потерпевших. Как правило, такими лицами являются представители кредитно-финансовых организаций. Так, Л., являясь сотрудником ПАО «Сбербанк», совершал хищения денежных средств клиентов банка. Приговором суда Л. осужден по п. «г» ч. 3 ст. 158 УК РФ³;

5) посредством неправомерного доступа к банковскому счету потерпевшего и оформления кредита от его имени. Так, Б., убедившись, что за действиями никто не наблюдает, воспользовался мобильным телефоном своей матери, зашел в приложение «Сбербанк Онлайн» и оформил от ее имени кредит на общую сумму более 32 тыс. руб., после чего осуществил перевод полученных денежных средств на открытый на свое имя банковский счет. Указанные действия квалифицированы судом по п. «г» ч. 3 ст. 158 УК РФ⁴;

6) посредством доступа к телефонному аппарату с установленными мобильными приложениями, в которых для оплаты товаров, работ, услуг указана чужая банковская карта. Так, К. приобрела у неустановленного лица ранее украденный сотовый телефон «Самсунг», в котором обнаружила установленное мобильное приложение «Ozon» с привязанной для оплаты товаров чужой банковской картой ПАО «Сбербанк». С целью совершения хищения К. осуществила заказ товаров и

1 Приговор Ленинского районного суда г. Уфы Республики Башкортостан от 10.03.2025 по делу N 1-24/2025. URL: <https://clck.ru/3PNAxX> (дата обращения: 18.09.2025).

2 Приговор Сысертского районного суда (Свердловская область) от 24.02.2025 по делу N 1-74/2025. URL: <https://sudact.ru/regular/doc/ha16Ly0u3V1p/> (дата обращения: 27.11.2025).

3 Приговор Октябрьского районного суда г. Новосибирска от 01.11.2019 по делу N 1-545/2019. URL: https://oktiabrskiy-nsk.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=538229833&case_uid=95b88be7-8b4d-4f30-812f-f90db59eee06&delo_id=1540006 (дата обращения: 27.11.2025).

4 Приговор Кировского районного суда г. Красноярск от 26.01.2022 по делу N 1-36/2022. URL: https://kirovsk-krk.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=310856985&case_uid=06335c19-64e3-43f3-b660-b0d3f6931ced&delo_id=1540006 (дата обращения: 10.01.2026).



произвела их оплату денежными средствами, находившимися на банковском счете указанной банковской карты. За совершение хищения К. осуждена по п. «г» ч. 3 ст. 158 УК РФ¹.

Резюмируя, необходимо также указать, что в зависимости от способа получения доступа к банковским картам, мобильным телефонам с установленными банковскими приложениями и т.п., используемыми для совершения хищения, возможна дополнительная квалификация действий преступника по ст. 158, ст. 161 УК РФ.

Приведенный в статье перечень способов совершения краж с использованием ИТТ является не полным и может дополняться в

процессе совершенствования подходов к реализации преступных намерений. При этом надеемся, что обозначенные проблемные вопросы в квалификации краж, отграничении их от смежных составов, а также приведенный перечень типичных способов совершения рассмотренных видов хищений, проиллюстрированный практическими примерами, будут способствовать уяснению сути деяний, их правильной квалификации, формированию единообразной судебной практики и повышению эффективности противодействия преступлениям, совершаемым с использованием ИТТ.

1 Приговор Белорецкого межрайонного суда Республики Башкортостан от 26.06.2025 N 1-228/2025. URL: <https://sudact.ru/regular/doc/m4pD14FDVAla/>. (дата обращения: 12.01.2026).

Библиографический список

1. Гайдин, А.И. Методика установления субъектов электронных платежей при расследовании хищений денежных средств : методические рекомендации / А.И. Гайдин, Е.А. Пидусов, А.В. Головчанский. – Воронеж: Воронежский институт МВД России, 2018. – 43 с.
2. Гумаров, И.А. Основы борьбы с кражами с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 Уголовного кодекса Российской Федерации) / И.А. Гумаров, Н.М. Сафин. – Казань : Казанский юридический институт МВД России, 2024. – 96 с.
3. Князьков, А.С. Криминалистическая характеристика преступления в контексте его способа и механизма / А.С. Князьков // Вестник Томского государственного университета. Право. – 2011. – N 1. – С. 51-64.
4. Маслиенко, М.А. Особенности квалификации краж и мошенничеств, совершаемых в информационно-телекоммуникационных сетях / М.А. Маслиенко // Проблемы правоохранительной деятельности. – 2023. – N 4(54). – С. 46-52.
5. Рускевич, Е.А. Отграничение мошенничества с использованием электронных средств платежа (ст. 159.3 УК РФ) от смежных составов преступлений / Е.А. Рускевич // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2022. – N 10(98). – С. 118-126.
6. Харина, Е.А. Некоторые аспекты квалификации мошенничества в сфере компьютерной информации / Е.А. Харина // Российский следователь. – 2022. – N 6. – С. 38-41.
7. Христюк, А.А. Проблемы уголовно-правовой регламентации и квалификации деяний, совершаемых с использованием электронных средств платежа / А. А. Христюк, Х. А. Асатрян // Академический юридический журнал. – 2023. – Т. 24. – N 1(91). – С. 71-79.
8. Хромов, Е.В. Проблемы квалификации хищения денежных средств с банковского счета / Е.В. Хромов // Уголовное право. – 2023. – N 2(150). – С. 44-58.