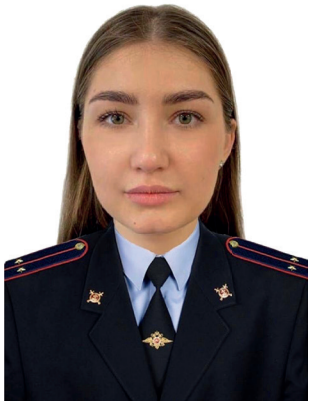
Научная статья
УДК 343.7
DOI: 10.37973/VESTNIKKUI-2025-59-7



ОБЪЕКТИВНЫЕ ПРИЗНАКИ ЦИФРОВОГО МОШЕННИЧЕСТВА И ИХ ЗНАЧЕНИЕ ДЛЯ КВАЛИФИКАЦИИ ДЕЯНИЯ

Диана Марсовна Ибатуллина,
Казанский юридический институт МВД России, Казань, Россия,
Zaxirova.diana@bk.ru

Аннотация

Введение*:* в статье рассматриваются понятие и сущность цифрового мошенничества; изучается понятие «цифровое мошенничество»; исследуются объект, а также обязательные и факультативные признаки объективной стороны цифрового мошенничества. При этом в статье анализируется как основной состав мошенничества, регламентированный ст. 159 УК РФ, так и квалифицированные составы (ст. 159^3 УК РФ, ст. 159^6 УК РФ). Автор исследует особенности установления отдельных признаков объективной стороны и указывает, что научную полемику вызывает вопрос определения информационных технологий как самостоятельного признака цифрового мошенничества, а также вопрос определения места совершения исследуемого противоправного явления.

Обзор литературы: изучены научные труды Д.В. Пучкова, Е.А. Русскевича, И.Р. Бегишева, Д.А. Овсюкова, М.А. Ефремовой, Е.В. Зотиной.

Материалы и методы: методологическая основа исследования представлена совокупностью общенаучных и специальных методов научного познания, среди которых диалектический метод, формально-юридический и системно-структурный метод. Эмпирическую основу исследования составили: действующие законодательные нормы, статистические данные ГИАЦ МВД России, постановления Пленума Верховного Суда Российской Федерации, постановления районных судов, представленные в открытых источниках.

Результаты исследования: автор приходит к выводу, что информационные технологии следует признавать именно средством совершения цифрового мошенничества, а местом совершения данных деяний необходимо считать местонахождение виновного лица.

Обсуждение и заключение: обосновывается необходимость дополнения ст. 159, ст. 159^3, ст. 159^6 УК РФ примечаниями, согласно которым размер значительного ущерба будет равен сумме не менее десяти тысяч рублей; а также дополнения ч. 3 ст. 159 УК РФ квалифицирующим признаком «с использованием информационных технологий», что, в свою очередь, позволит подчеркнуть повышенную общественную опасность подобных деяний и закрепить в законодательстве самостоятельный вид мошенничества с применением информационных технологий любого вида.

Ключевые слова: уголовное право; цифровое мошенничество; информационные технологии; объект; объективная сторона; средство; место совершения преступления

© Ибатуллина Д.М., 2025

Для цитирования: Ибатуллина Д.М. Объективные признаки цифрового мошенничества и их значение для квалификации деяния // Вестник Казанского юридического института МВД России. 2025. Т. 16. № 1 (59). С. 66 – 73. DOI: 10.37973/VESTNIKKUI-2025-59-7

Scientific article
UDC 343.7
DOI: 10.37973/VESTNIKKUI-2025-59-7

OBJECTIVE SIGNS OF DIGITAL FRAUD AND THEIR SIGNIFICANCE FOR THE QUALIFICATION OF THE ACT

Diana Marsovna Ibatullina,
Kazan Law Institute of the Ministry of Internal Affairs of Russia, Kazan, Russia,
Zaxirova.diana@bk.ru

Abstract

Introduction: the article considers the object and mandatory signs of the objective side of digital fraud (socially dangerous act, causal relationship and consequences), as well as optional signs (method, time, place, instrument, means of committing a criminal act, situation). At the same time, the article analyzes both the main composition of fraud, regulated by Article 159 of the Criminal Code of the Russian Federation, and qualified formulations (Article 159^3 of the Criminal Code of the Russian Federation, Article 159^6 of the Criminal Code of the Russian Federation). The author examines the peculiarities of establishing individual signs of the objective side and points out that the scientific controversy is caused by the question of defining information technology as an independent sign of digital fraud, as well as the question of determining the place of commission of the studied illegal phenomenon.

Literature review: the scientific works of Puchkov D.V., Russkevich E.A., Begishev I.R., Ovsyukov D.A., Efremov M.A. have been studied.

Materials and Methods: the methodological basis of the study is represented by a set of general scientific and special methods of scientific cognition, including the dialectical method, formal legal and systemic structural method. The empirical basis of the study was made up of: current legislative norms, statistical data of the GIAC of the Ministry of Internal Affairs of Russia, resolutions of the Plenum of the Supreme Court of the Russian Federation, resolutions of district courts presented in open sources.

Results: the author comes to the conclusion that information technology should be recognized as a means of committing digital fraud, and the location of the perpetrator should be considered the place of commission of these acts.

Discussion and Conclusions: in addition, it is determined that Part 3 of Article 159 of the Criminal Code of the Russian Federation should be supplemented with a qualifying feature "using information technology", which in turn will emphasize the increased danger of such acts and clearly define a single qualification for fraud using any type of information technology.

Keywords: criminal law; digital fraud; information technology; object; objective side; means; place of crime

© Ibatullina D.M., 2025

For citation: Ibatullina D.M. Objective Signs of Digital Fraud and Their Significance for the Qualification of the Act. Bulletin of the Kazan Law Institute of MIA of Russia. 2025;16(1):66-73. (In Russ.). DOI: 10.37973/VESTNIKKUI-2025-59-7

Введение

Сегодня обществу присущи чрезвычайно высокие темпы развития, особенно в сфере информационных технологий (IT). Технологическое влияние не только видоизменило привычный мир и способы коммуникации, но и стало неким «катализатором» преступлений. Информационные технологии активно применяются с противоправным умыслом, что уже повлекло за собой появление новых видов преступлений, посягающих на совершенно разные объекты, охраняемые уголовным законом: цифровое мошенничество, кибертерроризм, кибербуллинг и т.д.

Обзор литературы

Вопросы квалификации и уголовной ответственности цифрового мошенничества являются предметом научных исследования множества авторов. Так, среди известных научных деятелей в данном направления следует выделить И.Р. Бегишева [1], Д.А. Овсюкова [2], М.А. Ефремову [3], Д.В. Пучкова Д.В. [4], Е.А. Русскевича [5].

Материалы и методы

Методологическую основу исследования составили общенаучные методы: анализ и диалектический метод; специальные методы: формально-юридический и системно-структурный

методы. Эмпирическую основу исследования составили действующие законодательные нормы, статистические данные ГИАЦ МВД России, постановления Пленума Верховного Суда Российской Федерации, постановления районных судов, представленные в открытых источниках Отметим, что актуальность и чрезвычайную важность проблемы подтверждают не только научные исследования, но и эмпирические материалы, в частности, ежегодная сводка зарегистрированных преступлений, составляемая ГИАЦ МВД России.

Результаты исследования

С 2019 года в отчетных данных МВД России появился новый признак, определяющийся как «преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации», к данной группе относится и мошенничество, а именно ст. 159 УК РФ, 159^3 УК РФ, 159^6 УК РФ. Так, в 2020 году было зарегистрировано 237074 фактов, в 2021 году 249249 фактов, в 2022 году 257606 фактов.[1] Следовательно, мы можем говорить о формировании негативной тенденции увеличения фактов совершения мошенничества с использованием информационных технологий.

В исследовании мы ставим своей целью научно-теоретический анализ понятия «цифровое мошенничество», а также обзорный анализ особенностей объекта и объективных признаков цифрового мошенничества.

В доктрине уголовного права нет единого подхода к определению мошенничества, совершаемого с использованием информационных технологий. Ряд авторов включает данную группу в киберпреступления [6, с. 28], другие определяют данные преступления термином «цифровое мошенничество» [7, с. 61], иные определяют как «дистанционное мошенничество» [8, с. 22].

Однако киберпреступления охватывают значительное число преступлений, посягающих не только на чужую собственность, но и на другие объекты, охраняемые УК РФ, в частности, компьютерную информацию, конституционные права и свободу человека и гражданина и т.д. Мы считаем, что данный термин искусственно расширен. Дистанционное мошенничество предполагает отсутствие прямого контакта между виновным и потерпевшим, цифровое же мошенничество не исключает непосредственного контакта, но указывает на наличие информационных технологий при реализации преступного умысла.

На наш взгляд, группа исследуемых составов должна быть обозначена именно как «цифровое мошенничество», о котором в своих исследованиях упоминают К.К. Борзунов, З.В. Глухова, А.Ю. Сергеев и другие исследователи. Как отмечает Е.В. Зотина, развитие информационных технологий обусловило, помимо наличия ст. 159 УК РФ, введение в УК РФ специальных, квалифицированных составов – 159^3 УК РФ и ст. 159^6 УК РФ [9].

С нашей точки зрения, под цифровым мошенничеством следует понимать негативное противоправное явление, заключающееся в хищении чужого имущества путем обмана или злоупотребления доверием, реализуемое с использованием информационных технологий. В свою очередь, под информационными технологиями следует понимать процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Объект цифрового мошенничества идентичен родовому объекту, то есть это общественные отношения в сфере охраны собственности, а именно чужого имущества или права на него. Исследования не выделяют дополнительный объект цифрового мошенничества, мы же считаем, что дополнительным объектом цифрового мошенничества следует признавать информационную безопасность, поскольку преступными действиями виновное лицо нарушает работу информационной инфраструктуры, что само по себе в ряде случаев требует дополнительной квалификации по соответствующим статьям гл. 28 УК РФ (Преступления в сфере компьютерной информации), затрудняя установление признаков преступления для правоприменителя.

Имеются существенные различия в понимании предмета цифрового мошенничества, которым, в отличие от классического мошенничества, в рамках ст. 159 УК РФ, выступают не просто конкретизированные предметы материального мира, а электронные денежные средства или иные цифровые ресурсы, что подтверждается многочисленными примерами следственной и судебной практики. Так, например, предметами цифрового мошенничества становятся криптовалюта, виртуальные купоны, карты, подарочные сертификаты, NFT-объекты.

Предметом мошенничества признают конкретизированные предметы материального мира. Предметом же цифрового мошенничества в большинстве случаев являются именно электронные

[1] Состояние преступности в Российской Федерации за 2022 г. (архивные данные). URL: https://мвд.рф/reports/item/35396677/ (дата обращения: 13.11.2024).

денежные средства или иные цифровые ресурсы, что подтверждает и судебная практика.

Пример из практики: у П. появились сведения с паспортными данными К., после чего у него возник преступный умысел на хищение денежных средств. На основании имеющихся паспортных данных П. установил номер банковской карты и абонентский номер К., после чего, посредством услуги «Мобильный банк» совершил хищение денежных средств с помощью дистанционной транзакции в размере 12 тыс. рублей.

Центральный районный суд г. Челябинска признал П. виновным по ч. 2 ст. 159[6] УК РФ и назначил ему наказание в виде лишения свободы на срок два года.[1]

Виновный Х. убедил потерпевшую, что она должна взять деньги в кредит для приобретения у него криптовалюты по выгодной цене. Потерпевшая взяла кредитов на 3,5 миллиона рублей, передала денежные средства с целью приобретения криптовалюты. Виновный, получив денежные средства в особо крупном размере, скрылся.[2]

Безусловно, цифровое мошенничество предполагает и наличие потерпевшего лица.

Действующее уголовное законодательство не содержит понятия «объективная сторона преступления». Однако логика построения уголовно-правовых норм свидетельствует о необходимости наличия самого деяния для дальнейшего применения статьи Уголовного кодекса Российской Федерации, а в отдельных случаях о необходимости совокупности элементов: деяния, причинно-следственной связи и последствий.

В доктрине уголовного права все противоправные деяния по конструкции объективной стороны подразделяются на материальные и формальные составы.

Укажем, что как основной, так и квалифицированные составы мошенничества относятся к категории материальных составов, следовательно, для установления целостной объективной стороны деяний требуется исследовать три обязательных элемента: общественно опасное деяние, последствия, причинно-следственную связь.

Общественно опасное деяние заключается исключительно в действиях.

Отличительным признаком объективной стороны мошенничества выступает способ (обман или злоупотребление доверием), для данных составов он является обязательным.

Диспозиция ст. 159[3] УК РФ не умаляет реализации деяния путем обмана или злоупотребления, однако дополнительным признаком устанавливает использование электронных средств платежа.

Как отмечают исследователи, объективная сторона ст. 159[6] УК РФ отличается уникальностью. Законодатель, сохранив общие признаки мошенничества, указал иные способы совершения преступления: 1) ввод, удаление, блокирование, модификация компьютерной информации; 2) иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Научную полемику вызывает вопрос о способе совершения цифрового мошенничества, поскольку данный вид хищения сопряжен с использованием информационно-телекоммуникационных технологий, в том числе сети Интернет.

А.Е. Боронина полагает, что использование цифровых ресурсов является самостоятельным способом совершения преступления и нарушает общественные отношения в сфере информационной безопасности. [10, с. 255]

А.В. Сыпачев указывает, что самостоятельными способами следует признавать всю разновидность противоправных посягательств в виртуальном пространстве, к примеру, фишинг, смс-рассылки и т.д. [11, с. 4]

Некоторые ученые выдвигают противоположную точку зрения. К примеру, Г.А. Гундерич указывает, что в ст. 159[6] УК РФ законодатель применяет метод сочетания обмана и использования информационных технологий, поскольку способом в данном случае выступает «обман путем ввода, удаления, блокирования, модификации компьютерной информации…» [12, с. 13]

Однако, по нашему мнению, признание в данном случае информационных технологий в качестве способа некорректно, поскольку п. 20 постановления Пленума Верховного Суда Российской Федерации № 48 указывает, что «мошенничество в сфере компьютерной информации … требует дополнительной квалификации по ст. 272, ст. 273 или ст. 274.1 УК РФ»[3], а следовательно, интегрировать в единый способ вышеуказанные действия нельзя.

[1] Приговор Центрального районного суда г. Челябинска № 1-221/2017. СПС «КонсультантПлюс» (дата обращения: 12.11.2024).

[2] Апелляционное определение Московского городского суда от 31.05.2021 по делу № 10-6555/2021. СПС «КонсультантПлюс» (дата обращения: 12.11.2024).

[3] 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). СПС «Консультант Плюс» (дата обращения: 14.11.2024).

Информационные технологии однозначно не могут быть признаны и орудием совершения преступления, так как в уголовно-правовой доктрине орудиями принято признавать материальные вещи. Отвечая на вопрос о применении орудий, можно признать данным факультативным признаком сам персональный компьютер (ПК) и его отдельные периферийные устройства, но не информационные технологии как программные приемы.

На наш взгляд, использование информационных технологий следует признать средством совершения преступления. Ранее мы указывали, что информационные технологии действительно выступают своеобразным «проводником» от преступника к потерпевшему, то есть с помощью информационных технологий преступник может в наиболее короткий срок найти потенциальную жертву или расширить круг потерпевших, распространяя свою преступную деятельность, к примеру, в социальных сетях.

Цифровое мошенничество, в особенности посягающее на государственный сектор или финансовые правоотношения, влечет значительный ущерб для государства, нарушая целостную систему информационного безопасности страны и отдельных государственных систем.

Совершение исследуемых деяний влечет и наступление негативных последствий и для потерпевшего, в виде материального (имущественный) и морального ущерба.

На основании пункта 2 примечания 1 к ст. 158 УК РФ значительным ущербом в рамках исследуемых составов признается сумма более пяти тысяч рублей. Пункт 4 примечания 1 той же статьи устанавливает, что крупным размером признается стоимость имущества, превышающая двести пятьдесят тысяч рублей, особо крупным – один миллион рублей.

На наш взгляд, сумма, установленная в рамках п. 2 примечания 1 ст. 158 УК РФ не коррелирует с реальными размерами ущерба, а также с уровнем инфляционных процессов, реальной покупательской способностью рубля и других экономических тенденций. Предлагаем внести в ст. 159, ст. 159^3, ст. 159^6 УК РФ примечания, согласно которым размер значительного ущерба будет равен сумме не менее десяти тысяч рублей.

Причинно-следственная связь указывает на взаимосвязь между реализуемым деянием и наступившими последствиями, то есть, например, между обманом потерпевшего лица и причинением ему материального ущерба.

Переходя к анализу факультативных признаков объективной стороны, нам важно прийти к собственному аргументированному выводу о том, чем являются информационные технологии при совершении мошенничества.

Диспозиции ст. 159 УК РФ и ст. 159^3 УК РФ, ст. 159^6 УК РФ уже содержат разновидности способов совершения преступления: 1) обман; 2) злоупотребление доверием (предполагает использование доверительных отношений с потерпевшим в корыстных целях); 3) ввод, удаление, блокирование, модификация компьютерной информации … (на основании постановления Пленума Верховного Суда Российской Федерации),[1] то есть из позиции законодателя и Верховного Суда Российской Федерации следует, что данные составы уже обладают самостоятельными способами как элементами объективной стороны.

Вопрос установления места совершения мошенничества с использованием информационных технологий в научном сообществе до сих пор остается спорным. По данному вопросу ученые подразделяются на три основные группы:

Одни полагают, что местом совершения цифрового мошенничества следует признавать местонахождение банка или иного объекта, из которого были выведены денежные средства. К примеру, Г.Д. Бадзгарадзе считает, что местом совершения преступления, совершенного с информационными технологиями (на примере мошенничества), будет признано фактическое местонахождения банка, из которого были выведены денежные средства. [13, с. 162].

Другие ученые высказывают мнение о том, что местом совершения цифрового мошенничества необходимо признавать виртуальное пространство. А.А. Протасевич А.А. и Л.П. Зверянская придерживаются данной точки зрения и считают, что местом совершения подобных преступлений является само интернет-пространство. [14, с. 31]

Третью группу составляют ученые, указывающие, что местом совершения преступления необходимо признавать местонахождение виновного лица. Данной позиции придерживаются Н.И. Малыхина и С.В. Кузьмина [15, с. 244]

Отметим, что Пленум Верховного Суда Российской Федерации определил, что местом совершения киберпреступлений следует считать именно место совершения преступления, откуда действовал преступник. Мы считаем, что данная

[1] 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). СПС «Консультант Плюс» (дата обращения: 14.11.2024).

позиция гармонично дополняет нормы уголовно-процессуального законодательства[1].

Завершая анализ объективной стороны цифрового мошенничества, важно учитывать, что данные деяния могут быть совершены только в форме действий. При этом для объективной стороны анализируемых преступлений обязательными элементами выступают способ, последствия (материальные и моральные), причинно-следственная связь.

Ежегодный прирост цифрового мошенничества требует закрепления данного феномена в законодательном поле. Мы предлагаем дополнить ч. 3 ст. 159 УК РФ квалифицирующим признаком «с использованием информационных технологий», что, в свою очередь, позволит подчеркнуть повышенную опасность подобных деяний (значительные трудности при установлении объективных признаков преступления и расследовании такого рода преступлений).

Для правоприменителя важно обозначить разграничение предлагаемого нами нововведения от действующей редакции п. «г» ч. 3 ст. 158 УК РФ. В п. «г» ч. 3 ст. 158 УК РФ упоминаются электронные средства платежа, которые включают в себя только денежные средства как предмет преступного посягательства, в рамках предлагаемых изменений в п. 3 ст. 159 УК РФ мы говорим о любых способах и цифровых ресурсах, используемых для совершения мошенничества, в том числе и о широком круге предметов цифрового посягательства.

Обсуждение и заключение

При установлении объективных признаков цифрового мошенничества возникает ряд сложных аспектов, которые следует учитывать при установлении признаком преступления:

1. Под цифровым мошенничеством следует понимать негативное противоправное явление, заключающееся в хищении чужого имущества или приобретении права на чужое имущество путем обмана или злоупотребления доверием, реализуемом с использованием информационных технологий.

2. Под информационными технологиями для целей использования ст. 159 УК РФ и др. следует понимать процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

3. Цифровое мошенничество сопряжено с использованием виновным информационных технологий, которые следует рассматривать в качестве средства совершения противоправного деяния, поскольку именно их как процессы внешнего мира виновный использует для воздействия на объект преступления.

4. Сложности вызывает и установление такого признака противоправного деяния, как место совершение преступления. При установлении объективной стороны цифрового мошенничества, на наш взгляд, под местом совершения преступления следует понимать именно местонахождение виновного лица.

5. Предлагаем внести в ст. 159, ст. 159^3, ст. 159^6 УК РФ примечания, согласно которым размер значительного ущерба будет равен сумме не менее десяти тысяч рублей.

6. Предлагаем дополнить ч. 3 ст. 159 УК РФ квалифицирующим признаком «с использованием информационных технологий», что позволит подчеркнуть повышенную опасность подобных деяний (значительные трудности при установлении объективных признаков преступления и расследовании такого рода преступлений).

СПИСОК ИСТОЧНИКОВ

1. Бегишев И.Р. Понятие и виды преступлений в сфере обращения цифровой информации: дис. … канд. юрид. наук: 12.00.08. Казань, 2017. 204 с.

2. Овсюков Д.А. Корыстные преступления против собственности с использованием информационно-телекоммуникационных сетей: вопросы квалификации: дис. … канд. юрид. наук: 5.1.4. Москва, 2023. 231 с.

3. Ефремова М.А. Уголовно-правовая охрана информационной безопасности: дис. … д-ра юрид. наук: 12.00.08. Москва, 2018. 427 с.

4. Пучков Д.В. Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств: проблемы теории и практики: дис. … д-ра юрид. наук: 5.1.4. Екатеринбург, 2022. 474 с.

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37. СПС «КонсультантПлюс» (дата обращения: 14.11.2023).

5. Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дис. … д-ра юрид. наук: 12.00.08. Москва, 2021. 521 с.
6. Иванова Л.В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1. С. 25 – 33.
7. Сергеев А.Ю., Широкова О.В. Мошенничество в цифровом обществе в условиях социальных изменений // Цифровая социология. 2023. № 1. С. 59 – 71.
8. Давыдов В.О., Тишутина И.В. Цифровые следы в расследовании дистанционного мошенничества // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 3. С. 20 – 27.
9. Зотина Е.В. Мошенничество с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии: криминологическое исследование: дис. … канд. юрид. наук: 5.1.4. Казань, 2024. 249 с.
10. Боронина А.Е. Использование информационных технологий как способ совершения хищения // Вестник науки. 2023. № 11. С. 252 – 257.
11. Сыпачев А.Ю. Основные способы хищений с использованием сети Интернет // Концепт. 2019. № 10. С. 1 – 6.
12. Гундерич Г.А. Использование информационных технологий в качестве способов совершения преступления // Противодействие правонарушениям, совершаемым с использованием информационных технологий: сборник статей по материалам научно-практической конференции (III школы-семинара молодых ученых-юристов). Москва, 2020. С. 11 – 17.
13. Бадзгарадзе Г.Д. Вопросы установления места совершения мошенничества, осуществленного с использованием информационных технологий: криминалистический и уголовно-процессуальный аспекты // Сибирское юридическое обозрение. 2022. № 2. С. 157 – 163.
14. Протасевич А.А., Зверянская Л.П. Борьба с киберпреступностью как актуальная задача современной науки // Всероссийский криминологический журнал. 2011. № 3 (17). С. 28 – 33.
15. Малыхина Н.И., Кузьмина С.В. Алгоритм действий следователя в типовых ситуациях расследования мошенничеств, совершенных с использованием сети Интернет // Вестн. Том. гос. ун-та. 2021. № 462. С. 238 – 247.

REFERENCES

1. Begishev I.R. Ponyatie i vidy prestuplenij v sfere obrashcheniya cifrovoj informacii: dis. … kand. yurid. nauk: 12.00.08. Kazan', 2017. 204 s.
2. Ovsyukov D.A. Korystnye prestupleniya protiv sobstvennosti s ispol'zovaniem informacionno-telekommunikacionnyh setej: voprosy kvalifikacii: dis. … kand. yurid. nauk: 5.1.4. Moskva, 2023. 231 s.
3. Efremova M.A. Ugolovno-pravovaya ohrana informacionnoj bezopasnosti: dis. … d-ra yurid. nauk: 12.00.08. Moskva, 2018. 427 s.
4. Puchkov D.V. Ugolovno-pravovaya model' zashchity telekommunikacij ot prestupnyh posyagatel'stv: problemy teorii i praktiki: dis. … d-ra yurid. nauk: 5.1.4. Ekaterinburg, 2022. 474 s.
5. Russkevich E.A. Differenciaciya otvetstvennosti za prestupleniya, sovershaemye s ispol'zovaniem informacionno-kommunikacionnyh tekhnologij, i problemy ih kvalifikacii: dis. … d-ra yurid. nauk: 12.00.08. Moskva, 2021. 521 s.
6. Ivanova L.V. Vidy kiberprestuplenij po rossijskomu ugolovnomu zakonodatel'stvu // Yuridicheskie issledovaniya. 2019. № 1. S. 25 – 33.
7. Sergeev A.Yu., Shirokova O.V. Moshennichestvo v cifrovom obshchestve v usloviyah social'nyh izmenenij // Cifrovaya sociologiya. 2023. № 1. S. 59 – 71.
8. Davydov V.O., Tishutina I.V. Cifrovye sledy v rassledovanii distancionnogo moshennichestva // Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki. 2020. № 3. S. 20 – 27.
9. Zotina E.V. Moshennichestvo s ispol'zovaniem informacionno-telekommunikacionnyh tekhnologij i priemov social'noj inzhenerii: kriminologicheskoe issledovanie: dis. … kand. yurid. nauk: 5.1.4. Kazan', 2024. 249 s.
10. Boronina A.E. Ispol'zovanie informacionnyh tekhnologij kak sposob sovershheniya hishcheniya // Vestnik nauki. 2023. № 11. S. 252 – 257.
11. Sypachev A.Yu. Osnovnye sposoby hishchenij s ispol'zovaniem seti Internet // Koncept. 2019. № 10. S. 1 – 6.

12. Gunderich G.A. Ispol'zovanie informacionnyh tekhnologij v kachestve sposobov sovershenija prestupleniya // Protivodejstvie pravonarusheniyam, sovershaemym s ispol'zovaniem informacionnyh tekhnologij: sbornik statej po materialam nauchno-prakticheskoj konferencii (III shkoly-seminara molodyh uchenyh-yuristov). Moskva, 2020. S. 11 – 17.
13. Badzgaradze G.D. Voprosy ustanovleniya mesta sovershenija moshennichestva, osushchestvlennogo s ispol'zovaniem informacionnyh tekhnologij: kriminalisticheskij i ugolovno-processual'nyj aspekty // Cibirskoe yuridicheskoe obozrenie. 2022. № 2. S. 157 – 163.
14. Protasevich A.A., Zveryanskaya L.P. Bor'ba s kiberprestupnost'yu kak aktual'naya zadacha sovremennoj nauki // Vserossijskij kriminologicheskij zhurnal. 2011. № 3 (17). S. 28 – 33.
15. Malyhina N.I., Kuz'mina S.V. Algoritm dejstvij sledovatelya v tipovyh situaciyah rassledovaniya moshennichestv, sovershennyh s ispol'zovaniem seti Internet // Vestn. Tom. gos. un-ta. 2021. № 462. S. 238 – 247.

Информация об авторе:
Ибатуллина Диана Марсовна, адъюнкт Казанского юридического института МВД России, zaxirova.diana@bk.ru
Автор прочитал и одобрил окончательный вариант рукописи.

Information about the author:
Ibatullina Diana M., Postgraduate of the Kazan Law Institute of the Ministry of Internal Affairs of Russia, zaxirova.diana@bk.ru
The author has read and approved the final version of the manuscript.

Статья получена: 20.01.2025.
Статья принята к публикации: 25.03.2025.
Статья опубликована онлайн: 27.03.2025.
Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.