DOI 10.37882/2223-2974.2025.09.10

СОЦИАЛЬНО-ПРАВОВЫЕ ДЕТЕРМИНАНТЫ КРИМИНАЛИЗАЦИИ И ПЕНАЛИЗАЦИИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В СОВРЕМЕННОЙ РОССИИ

SOCIAL AND LEGAL DETERMINANTS OF CRIMINALIZATION AND PENALIZATION OF COMPUTER-TERM INFORMATION FRAUD IN MODERN RUSSIA

Yu. Ivanov

Summary. In the modern world, digital technologies affect all spheres of life, which makes criminal liability for fraud in the field of computer information especially relevant. The increase in electronic information transactions expands the possibilities of fraud, which negatively affects Russia's national security.

The purpose of the article is to identify the main factors that have led to criminal liability and punishment for fraudulent actions in the field of computer information in order to improve strategies to combat this type of crime in modern Russia.

The main tasks are to identify and analyze the objective factors that led to the establishment of criminal liability and to identify the determinants that contribute to the emergence of criminal risks.

An integrated approach was used in the work, including: general scientific methods: dialectical, statistical; and specialized methods: comparative analysis, system-structural analysis, sociological analysis and content analysis.

The study identifies and analyzes key factors contributing to the criminalization and criminalization of fraud in the field of digital data, and finds that the rapid development of IT technologies, Internet services, and online platforms expands opportunities for attackers and increases the complexity of law enforcement.

Keywords: fraud, computer information, digital data sphere, social conditioning, penalization, determinants.

Иванов Юрий Владимирович
Аспирант, Юго-Западный государственный университет (Курск)
Dr.uriy-ivanov@yandex.ru

Аннотация. В современном мире цифровые технологии влияют на все сферы жизни, что делает уголовную ответственность за мошенничество в сфере компьютерной информации особенно актуальной. Увеличение электронных информационных транзакций расширяет возможности мошенничества, что негативно сказывается на национальной безопасности России.

Целями статьи обозначим определение основных факторов, которые обусловили уголовную ответственность и наказание за мошеннические действия в сфере компьютерной информации с целью улучшения стратегий борьбы с этим видом преступности в современной России.

Основными задачами выделим выявление и анализ объективных факторов, которые привели к установлению уголовной ответственности и определение детерминант, способствующих возникновению криминальных рисков.

В работе использовался комплексный подход, включающий: общенаучные методы: диалектический, статистический; и специализированные методы: сравнительный анализ, системно-структурный анализ, социологический анализ и контент-анализ.

В исследовании определены и проанализированы ключевые факторы, способствующие криминализации и установлению уголовной ответственности за мошенничество в сфере цифровых данных, установлено, что быстрое развитие IT-технологий, интернет-сервисов и онлайн-платформ расширяет возможности для злоумышленников и увеличивает сложность правоприменения.

Ключевые слова: мошенничество, компьютерная информация, сфера цифровых данных, социальная обусловленность, пенализация, детерминанты.

Век технологической революции принес изменения во все сферы: Создание самодостаточных и адаптивных программных комплексов (ИИ, автоматизированные системы), Эволюция экономики: глобальные связи, реформа финансовых институтов, расширение инвестиционно-страхового рынка, Появление новых рисков: sophisticated-мошенничество и схемы противоправного присвоения собственности.

Ученые подчеркивают, что современные технологические достижения в сфере электроники, софта и способами передачи информативных данных привлекают внимание преступников, активно использующих их в своих целях [1, с. 38]. Считается, что современная киберпреступность переросла в масштабную криминальную сферу, охватывающую «богатый выбор» противозаконных операций, от действий сексуальных извращенцев развращающих подрастающих молодых людей до кибервзломщиков, в том числе и разнообразных типов цифровых мошенников [2, с. 45]. Сегодня мошенничество, совершаемое с использованием компьютерных данных и интернет-сетей, является одним из самых распростра-

ненных преступлений в глобальном масштабе. Оценка масштабов и структуры преступности в сфере информационных технологий в России за период с 2002 по 2012 год выявил более 2800 вредоносных инцидентов в год, включая значительный рост (35 %) эпизодов обманов и злоупотреблений в сфере вычислительной техники и информации [3, с. 175].

Поэтому важно провести полный анализ социальных и правовых причин, влияющих на объективную оценку и выбор меры ответственности за мошенничество, особенно за его особые виды в цифровой сфере. Этот подход продиктован эволюцией экономических преступлений, в частности, увеличением числа и сложности новых видов мошеннических схем, использующих цифровые информационные технологии.

Для исследования проблемы применялись различные методы, в числе которых — диалектический. С его помощью были изучены условия, от которых зависит уголовное наказание за компьютерное мошенничество, а также предпосылки для увеличения таких преступлений в условиях российской системы property relations. Эмпирические и статистические методы, сравнительный анализ, синтез, дедукция и индукция: для изучения, обобщения и интерпретации ключевых обстоятельств, определяющие криминализацию и меру наказания за мошенничество в цифровом информационном пространстве, включая анализ криминальных рисков, связанных с мошенническими схемами в рассматриваемой информационной области.

Мы сравнили собранную информацию с текстом ст. 159.6 УК и схожими преступлениями. Выяснилось, что закон сложно применять на практике, и его формулировки противоречивы. На основе этого мы предложили, как можно улучшить эту статью уголовного кодекса.

В контексте экспоненциального умножения криминальной активности в онлайн-электронном пространстве, характеризующейся активным применением программного обеспечения, сетевых ресурсов и хранилищ информации, российскими правоведами и, впоследствии, законодателями были идентифицированы специфические черты киберпреступлений. Это позволило провести четкую демаркацию между пониманием того, какие действия и иными противоправные поступки с информационными технологиями, совершаемыми посредством цифровых устройств, являются законными, а какие нет.

Было установлено, что любое неправомерное использование компьютерной информации в преступных целях неизбежно приводит к деструктивному воздействию, выходу из строя или сбоям в работе компьютерных систем, а также связанных с ними электронных ресурсов, аппаратного обеспечения и информационных активов. В конечном счете, это подрывает безопасность компьютерной информации на всех этапах ее «жизненного цикла», угрожает её конфиденциальности, целостности и доступности в любое время и не зависимо от какой-либо определенной территории, что критически важно и актуально для предотвращения мошеннических сценариев [4, с. 833].

Для обеспечения безопасности графических пользовательских интерфейсов, программ и хранилищ платформ информационных потоков, 23 сентября 1992 года в Российской Федерации был принят Федеральный закон № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных». Указанный законодательный акт сформировал базовую правовую структуру, обеспечивающую охрану программного обеспечения и отечественной информационной конфигурации.

Данный закон заложил правовой фундамент для защиты программного обеспечения и информационных систем от несанкционированного доступа и использования.

Помимо этого, он отнес к уголовно наказуемым деяниям хищение компьютерных программ и баз данных, а также их незаконное копирование и распространение, признав такие действия посягательством на интеллектуальную собственность.

В редакции Уголовного кодекса Российской Федерации 1996 года, о которой идет здесь речь, ответственность за рассматриваемые деяния определялась на основании статей, соответствующих родовому и видовому объектам преступного посягательства. При этом компьютерная информация квалифицировалась как орудие или средство совершения преступления.

При определенных условиях противоправная деятельность лица может образовывать объективную сторону нескольких составов. Так, если доступ к охраняемой информации получен с применением вредоносных программ, содеянное подлежит квалификации по совокупности всех трех статей главы 28 УК РФ.

Таким образом, сочетание статей 272-274 УК РФ позволяло более гибко подходить к расследованию преступлений в сфере компьютерной информации, охватывая различные аспекты и уровни вмешательства в информационные системы.

Правовая основа борьбы с IT-мошенничеством в России коренится в конституционных нормах. Конституция закрепляет право на свободный поиск и распространение информации (ст. 29), формирует правовые осно-

вы информационного пространства и разграничивает компетенцию в сфере инфотехнологий (ст. 71), а также обеспечивает равную защиту всех форм собственности, в том числе цифровой (ст. 8). Поправки 2020 года обозначили потребность в модернизации информационного законодательства. В развитие конституционных положений были приняты федеральные законы «Об информации, информационных технологиях и о защите информации» и «О персональных данных», которые детализируют и расширяют конституционные нормы, касающиеся защиты информации и противодействия киберпреступности.

Появление такого понятия обусловлено необходимостью решения проблем, возникающих в связи с ростом киберпреступности, и защищает права граждан и организаций на использование и хранение информации. Это определение стало основой для дальнейшего расширения и уточнения законодательства в сфере защиты информационных технологий. На основе этого определения разрабатывались такие инструменты, как законы о кибербезопасности и защите персональных данных, о которых речь шла выше.

Импульсом к изменению уголовного законодательства послужил поручение Президента РФ, данное Министерству юстиции и Министерству экономического развития. В соответствии с ним требовалось проанализировать и модернизировать статью 159 УК РФ (мошенничество) к 2012 году, а также изучить вопрос о расширении перечня видов обмана. Целью данной инициативы было повышение эффективности правоприменения, обеспечение единообразия в квалификации по ст. 159.6 УК РФ и пресечение злоупотреблений, связанных с пробелами в смежном законодательстве.

Установление более строгих санкций должно было стать сдерживающим фактором для предполагаемых правонарушителей. В рамках проекта был сделан акцент на превентивные меры, позволяющие не только реагировать на уже совершенные преступления, но и предотвращать их с помощью более четких норм и действий правоохранительных органов. Законопроект «О корректировке Уголовного кодекса Российской Федерации и других законодательных актов Российской Федерации» явился важным шагом в адаптации правовой системы к современным вызовам, связанным с мошенничеством. Разграничение видов мошеннических действий и уточнение их правовых характеристик должны повысить эффективность правоохранительной деятельности и усилить защиту прав граждан.

Проект закона также учитывает опыт зарубежного уголовного права, развитых стран и российские судебные решения по мошенничеству за 2011 год (данные ВС РФ). В УК РФ была имплементирована новая глава, дополненная статьями 159.1–159.6. Законодатель, вводя статью 159.6 УК РФ, стремился адаптировать уголовное законодательство к новым видам мошенничества, связанным с развитием цифровой среды и информационных систем.

Ещё до законодательного закрепления норм, регулирующих компьютерные преступления, и последующего введения статьи о мошенничестве в сфере компьютерной информации (ст. 159.6 УК РФ, введенной Федеральным законом от 07.12.2011 № 420-ФЗ), академическое сообщество проявляло повышенный интерес к противоправным действиям мошеннического характера, осуществляемым в информационных системах.

В двухтысячных годах учёные-юристы активно обсуждали, что нужно изменить Уголовный кодекс, чтобы подвести под статью «незаконное обогащение в крупных размерах с помощью компьютеров или интернета». [5, с. 10].

В академических трудах того периода предлагалось квалифицировать подобные действия либо как мошенничество в тесном смысле слова (ст. 159 УК РФ), определяя их через призму «получения выгоды с использованием компьютерной техники или ЭВМ» [6, с. 261], либо как неправомерное использование компьютерных данных для получения выгоды обманным путем, в соответствии с концепцией единства родового объекта деяний, закрепленных в главе 28 УК. [7, с. 85].

Часть научного сообщества указывала, что «противоправное извлечение преимуществ с помощью компьютерных систем» представляет собой неправомерное безвозмездное завладение имуществом в значительном размере, реализуемое при помощи средств вычислительной техники, что позволяет отнести указанные деяния к категории преступлений небольшой тяжести (в случаях, когда размер причиненного вреда не превышает 2500 рублей, имеет место административный проступок). [8, с 43].

Пленум Верховного Суда РФ в Постановлении № 48 от 30.11.2017 г. указал на необходимость квалификации мошенничества, совершенного с применением электронно-вычислительной техники, с учетом наличия квалифицирующих признаков, влияющих на тяжесть наказания.

Раньше в главе 28 УК РФ преступления связывали с конкретным «железом» — компьютерами, серверами, сетевым оборудованием. Поэтому, чтобы привлечь к ответственности за мошенничество в цифровой сфере (ст. 159 УК РФ), нужно было доказать использование такого оборудования.

До появления специального закона в 2011 году основой для всех определений служили именно эти «аппаратные» термины, и они подходили только для «обычных» преступлений.

Если понять, почему мошенничество с компьютерной информацией стало отдельным преступлением и какое наказание за него предусмотрели, становятся ясны основные цели законодателей. В контексте современной информационной среды, где информация является критически важным активом, наблюдается экспоненциальный рост киберпреступности. Если ранее подобные инциденты носили спорадический характер, то в настоящее время, считает С.С. Медведев, они интегрированы в структуру современной преступности [9, с. 172].

Таким образом, статья 159.6 УК РФ является необходимой реакцией на изменения в обществе и технологическом окружении, образуя правовую основу для борьбы с мошенническими действиями в условиях современной экономики и цифровизации.

По мнению ряда учёных, постоянное добавление новых норм говорит о стагнации уголовного права и тормозит его адаптацию к новым реалиям, когда предпочтение отдаётся количеству новых статей, а не качеству существующих.

Это даёт основания полагать, что государство стремится к излишнему регулированию. Подобный подход усложняет право, создаёт неопределённость и путает граждан и правоприменителей, особенно в IT-сфере. Исследователи видят в этом не развитие, а чрезмерный контроль, который лишает правовую систему гибкости и подрывает её способность эволюционировать, повышая уязвимость и снижая адаптивность законодательства. [10, с. 5 — 6].

Мы придерживаемся иной точки зрения. По нашему мнению, конкретизация мошенничества — это не причуда, а насущная потребность, вызванная появлением сложных схем преступной деятельности, повсеместной цифровизацией и расширением digital-пространства. Кроме того, она способствует упорядочиванию правоприменительной практики, повышая её эффективность.

Ранее звучали критические замечания о том, что новые формы мошенничества грозят избыточной бюрократизацией [11, с. 29]. Высказывались насчёт сложных формулировок, повторения норм и излишней казуистики [12, с. 61]. Встречалось мнение о бессмысленности таких нововведений из-за риска конфликта правовых норм [13, с. 19].

Тем не менее, утверждение о полной идентичности существующих статей о видах мошеннических действий и сопредельных с ними уголовно-правовых предписаний, на наш взгляд, выглядит поспешным. Злоумышленники, использующие безграничные возможности цифрового мира, могут вычислять и маскироваться под представителей официальных организаций, вводя в заблуждение всё большее количество граждан.

Ст. 159 УК РФ трактует мошенничество широко — как кражу собственности обманом или введением в заблуждение. Закон не перечисляет все возможные способы, подразумевая стандартные: при встрече, по телефону, через письма. Например, это фальсификация бумаг или недобросовестная сделка.

Мошенничество в традиционном понимании представляет опасность, однако в современных реалиях эта угроза может быть ощутимо ограничена в пространственном и временном аспектах.

В мошенничестве с использованием компьютерной информации (ст. 159.6 УК) могут применяться такие методы, как фишинг, использование вредоносного ПО, взлом аккаунтов, манипуляции с данными и другие формы электронного обмана, что создает совершенно иные риски и угрозы для общества, требующие специального подхода.

Цифровое мошенничество является сверхактуальной угрозой, ведь оно действует без границ, мгновенно и массово. Оно нацелено на хищение критически важной личной и финансовой информации, что влечёт за собой катастрофический ущерб. Совершение основного состава «классического» мошенничества, наказывается максимально, лишением свободы на срок до двух лет, а за мошенничество в сфере компьютерной информации максимальный срок наказания предусмотрен в виде ареста на срок до четырех месяцев.

В этом и содержатся принципиальные отличия, оправдывающие обновления и детализацию уголовного законодательства (криминализацию и пенализацию).

Следовательно, разграничение статей 159 и 159.6 УК РФ акцентирует потребность в применении специализированного подхода к противодействию мошенничеству в контексте динамично развивающегося технологического общества. В условиях трансформации преступных методик, уголовное право призвано адаптироваться для надлежащей защиты прав и интересов граждан.

Сущность рисков, согласующихся с рассматриваемым видом мошенничества, объясняется увеличением числа пользователей интернета и распространением технологий, из-за чего мошенничество в области компьютерных данных стало более распространенной

и опасной угрозой. Такой вид преступления может затрагивать как отдельных граждан, так и крупные компании, нанося ущерб их репутации и финансовым ресурсам.

Введение специальной статьи влечёт особые наказания за такие преступления, ужесточая ответственность за технологически обусловленное мошенничество, особенно его сложные формы, что подчёркивает его повышенную вредоносность.

Для каждого специального состава мошенничества действуют свои оценочные критерии. Так, ст. 159.1 УК РФ касается обмана в кредитной сфере, а ст. 159.6 УК РФ — манипуляций с компьютерной информацией.

Причины введения законодательства о компьютерном мошенничестве вызывают споры, но его актуальность для защиты собственности не оспаривается. Нам представляется, что следует акцентировать внимание на том, что внедрение защиты цифровых технологий в уголовно-правовую сферу привело к увеличению числа и усложнению характера киберпреступлений. Проникновение информационных технологий во все аспекты жизни общества делает эти преступления особенно опасными, а, следовательно, в перспективе, особо специфичные формы и виды деяний будут включены законодателем в УК РФ, как новые нормы.

Мы солидарны с Е.С. Лариной и В.С. Овчинским в том, что преступность — это искажённое зеркало технологических, социально-экономических и политических сдвигов. [14, с. 7].

Федеральный закон № 207-ФЗ разделил мошенничество на три типа: мошенничество в сфере компьютерной информации, которое теперь регулируется статьей 159.6 УК РФ, «обычное» мошенничество (ст. 159 УК) и все остальные виды мошенничества. Последние рассматриваются либо по общей статье 159 УК РФ, либо по специализированным статьям, таким как мошенничество в сфере кредитования (ст. 159.1), при получении выплат (ст. 159.2) и с использованием электронных средств платежа (ст. 159.3). Иными словами, вышеназванный документ акцентирует внимание на классификации мошеннических действий по видам, что обусловлено необходимостью улучшения эффективности предотвращения таких преступлений, которые стали довольно распространёнными и представляют угрозу как отдельным гражданам, так и обществу в целом, вызывая значительные убытки. В результате, уголовное законодательство было расширено новыми статьями, регулирующими ответственность за мошенничество в специфических областях цифровой деятельности, отличающихся эксклюзивной характеристикой посягательств и методами совершения преступлений.

Ряд юристов продолжает ставить под вопрос создания специальных норм о мошенничестве. По одной из точек зрения, можно было ограничиться модификацией старых статей (ст. 159 или гл. 28 УК РФ) [15, с. 81]. По другой — закон не успел за новыми видами обмана, и его нормы конфликтуют между собой, как, например, ст. 159.3 и 159.6 УК РФ [16, с. 26].

Мы категорически не согласны с этой критикой. На наш взгляд, сложностей в отграничении ст. 159.6 УК РФ от других составов нет. Пересечение со ст. 159.3 УК РФ есть, но развести их достаточно просто.

Более того, введение специализированных составов, особенно в области компьютерной информации и информационно-телекоммуникационных сетей, продиктовано социально-публичной необходимостью. Целью этих нововведений является не отграничение сфер мошеннической деятельности, а их оптимизация, корректировка, упорядочивание и регулирование.

В рамках рассматриваемой проблемы существуют как приверженцы принятой законодательной модели [17], так и её оппоненты [18], выдвигающие альтернативные предложения по совершенствованию ст. 159.6 УК РФ. Мы полагаем, что данная дискуссия подчёркивает злободневность нашего исследования и стимулирует его дальнейший анализ — как в теоретическом, так и в практическом ключе. Особую значимость этому придаёт тот факт, что правоприменительная практика по данному вопросу остаётся противоречивой. Этот аспект крайне важен, поскольку разрозненность судебных решений обнажает трудности, связанные с толкованием новелл уголовного закона, что, в свою очередь, требует от юристов и правоприменителей глубоких познаний в области цифровых технологий.

Статистика ЦБ за 2023 год показывает резкий скачок числа несанкционированных операций на 11,48 %, сигнализируя о новой волне мошенничества в банковской среде.

При этом на фоне общего роста карточных платежей на 10,54 % прослеживается и рост мошеннических схем, идущий рука об руку с увеличением числа транзакций.

Положительной новостью стало то, что банки вернули жертвам афер уже 8,7 % от всех похищенных сумм — это более чем в полтора раза выше, чем годом ранее (4,4 %).

Однако в 2024 году масштабы бедствия стали еще больше: fraudulent-операции выросли на ошеломляющие 74 %, заставляя регуляторов и банки срочно усиливать защиту и работать над возвратом денег гражданам и бизнесу.

По данным МВД, уже 40% всех преступлений в России — IT-преступления, то есть каждое четвертое правонарушение происходит в digital-пространстве. Увеличение на 13,1 % в сопоставлении с годом ранее показывает, что цифровые технологии становятся ключевым инструментом для совершения уголовных деяний. Более того, доля таких преступлений в общем количестве зарегистрированных случаев достигает 25 %, что акцентирует внимание на значимости и серьезности данной проблемы.

Согласно данным, представленным Банком России, в 2023 году наблюдался 11,48 %-ный рост несанкционированных операций, произведенных без ведома клиентов банков, по сравнению с 2022 годом. Это увеличение произошло на фоне общего роста оборота карточных денежных переводов, который составил 10,54 %, достигнув внушительной суммы в 136,38 триллиона рублей.

В 2023 году финансовые учреждения вернули своим клиентам лишь 1 378,8 миллиона рублей, что составляет 8,7 % от всей суммы несанкционированных денежных переводов, совершенных как физическими, так и юридическими лицами. Этот показатель значительно выше, чем в 2022 году, когда гражданам и юридическим лицам было возвращено всего 618,4 миллиона рублей, что составило 4,4 % от общего количества мошеннических случаев.

В 2024 году наблюдается значительный рост несанкционированных операций, осуществленных без ведома клиентов, который составил 74,36 % по сравнению с 2023 годом. Однако, несмотря на это увеличение, доля таких операций в общем объеме денежных переводов составила лишь 0,00066 %, что является снижением по сравнению с 2023 годом, при достижении этим показателем 0,00119 %.

В 2024 году был зафиксирован заметный увеличенный уровень преступлений, осуществляемых с применением информационных технологий и коммуникационных средств, а также в области компьютерных данных.

В минувшем году киберпреступность составила более двух пятых (40 %) всех зарегистрированных преступлений, что на 13,1 % больше, чем 2023 году. Особенно тревожным является рост тяжких и особо тяжких киберпреступлений, который составил 7,8 %. Данный фактор оказал значительное влияние на общую статистику серьезных (особо опасных) преступлений в стране, увеличив их число на 4,8 % в 2024 году.

Заключение

Подводя итоги социально-правового обоснования введения в УК РФ специальной статьи о компьютерном мошенничестве, необходимо отметить ключевую роль информационных систем и digital-пространства в современном обществе. Они гарантируют высокоскоростной обмен данными, что обуславливает особую важность их защиты. В то же время, повсеместное проникновение digital-технологий во все сферы жизни создаёт плодотворную почву для разнообразных форм противоправной деятельности. К их числу относится и мошенничество, осуществляемое путём несанкционированного доступа к персональным данным граждан, что формирует серьёзную угрозу национальной безопасности.

Эксперты считают, что нынешний курс уголовной политики нуждается в создании актуальных концепций и нормативных предложений, нацеленных на охрану компьютерных данных, которые должны быть согласованы с global-тенденциями, но при этом опираться на национальные приоритеты [19, с. 78].

Важно избегать недооценки растущей опасности имущественных преступлений, совершаемых в digital-среде. В некоторых случаях целесообразно ввести уголовную ответственность за действия, создающие серьёзные риски в контексте ускоренной digital-трансформации.

ЛИТЕРАТУРА

1. Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. 2012. № 2. С. 37–44.
2. Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. 2008. № 2. С. 44–46.
3. Комаров А.А. Компьютерное мошенничество в России и США: анализ количественных показателей за 2002-2012 гг. // Юридическая наука и правоохранительная практика. 2016 № 1 (35). С. 172–177.
4. Учебный комментарий к Уголовному кодексу Российской Федерации. Отв. ред. Жалинский А.Э. — М.: Изд-во Эксмо, 2005. 1088 с.
5. Безверхов А.Г. Развитие понятия мошенничества в отечественном праве // Уголовное право. 2001. № 4. С. 9–12.
6. Безверхов А.Г. Имущественные преступления. — Самара: Самар. ун-т, 2002. 359 с.
7. Бражник С.Д. Проблемы совершенствования норм об ответственности за преступления, связанные с компьютерной техникой // Налоговые и иные экономические преступления. Сборник научных статей. — Ярославль: Изд-во Яросл. ун-та, 2000. Вып. 2. С. 78–86.
8. Лопатина Т.М. Компьютерная преступность. Монография. — Смоленск: Универсум, 2006. 184 с.
9. Медведев С.С. Характеристика лица, совершающего компьютерное мошенничество // Экстремизм и другие криминальные явления. — М.: Российская криминологическая ассоциация, 2008. С. 171–174.
10. Болдырев В. Мошенничество с целью получения социальных выплат: предмет преступления // Уголовное право. 2014. № 3. С. 4–12.

11. Кленова Т.В. О разграничении смежных и конкурирующих составов преступлений (на примере мошенничества) // Уголовное судопроизводство. 2014. № 1. С. 25–30.
12. Шарапов Р.Д. Новые уголовно-правовые нормы об ответственности за мошенничество: инструмент реальной борьбы или бутафория закона? // Библиотека уголовного права и криминологии. 2013. № 3. С. 60–66.
13. Маркунцов С.А. О масштабах перманентной новеллизации Уголовного кодекса РФ // Законы России: опыт, анализ, практика. 2018. № 2. С. 18–26.
14. Ларина Е.С., Овчинский В.С. Криминал будущего уже здесь. М.: Кн. мир, 2018. 505, [2] с.
15. Перетолчин А.П. Актуальные способы мошенничества с использованием информационно-телекоммуникационных технологий // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: материалы Всероссийской научно-практической конференции. — Иркутск, 2021. С. 79–83.
16. Гладких В.И. Компьютерное мошенничество: а были ли основания его криминализации? // Российский следователь. 2014. № 22. С.25–31.
17. Абдульмянова Т.В., Асанова И.П., Данилов В.В. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ): понятие, уголовно-правовая характеристика и некоторые особенности расследования // Вопросы российского и международного права. 2021. Т. 11. № 1-1. С.134–145.
18. Гладких В.И. Эволюция норм об ответственности за мошенничество в российском уголовном законодательстве // Deutsche Internationale Zeitschrift für zeitgenössische Wissenschaft. 2021. № 10-2. С. 21–23.
19. Батурин Ю.М., Полубинская С.В. Совершенствование законодательных норм уголовно-правового цикла в контексте высокотехнологического будущего. В кн.: Преступность в XXI веке. Приоритетные направления противодействия: монография / под ред. А.Н. Савенкова. М.: ЮНИТИ-ДАНА: Закон и право, 2020. 559 с.