УДК 343.3/.7 DOI: 10.17277/pravo.2026.01.pp.099-107

КИБЕРПРЕСТУПНОСТЬ В СФЕРЕ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ: КВАЛИФИКАЦИЯ И ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ

Халимат Алиевна Аккаева, *канд. юрид. наук, доцент, заместитель начальника управления науки и инноваций, ФГБОУ ВО «Кабардино-Балкарский государственный аграрный университет имени В. М. Кокова», Нальчик, Кабардино-Балкарская Республика, Россия; akkaevah@mail.ru*

Приведен комплексный анализ проблем квалификации и противодействия киберпреступлениям в сфере банковской деятельности. Рассмотрены эволюция киберпреступности, ее специфика в банковском секторе, а также недостатки действующего уголовного законодательства России в части регламентации ответственности за данные деяния. Особое внимание уделено проблемам квалификации хищений, совершаемых с использованием электронных средств платежа, атак на объекты критической информационной инфраструктуры банков, а также неправомерного доступа к банковской тайне. Проанализированы различные научные подходы к решению данных проблем, а также предложены конкретные меры по совершенствованию законодательства и правоприменительной практики. Исследованы вопросы международного сотрудничества и зарубежного опыта в сфере борьбы с киберпреступностью в банковской сфере.

Ключевые слова: киберпреступность; банковская деятельность; электронные средства платежа; критическая информационная инфраструктура; банковская тайна; хищение; неправомерный доступ; квалификация преступлений; уголовная ответственность; международное сотрудничество.

Введение. Постановка проблемы

Стремительное развитие информационных технологий и их повсеместное внедрение во все сферы жизни общества, включая банковскую деятельность, обусловили появление нового вида преступности – киберпреступности. Киберпреступность в банковской сфере представляет собой серьезную угрозу не только для отдельных кредитных организаций и их клиентов, но и для финансовой стабильности государства в целом. Преступники используют все более изощренные методы атак, направленные на хищение денежных средств, получение неправомерного доступа к конфиденциальной информации, нарушение работы банковских систем.

В последние годы наблюдается значительный рост числа киберпреступлений, совершаемых в отношении банков и их клиентов. Так, по данным Банка России, объем операций без согласия клиентов в 2023 году вырос на 33 % по сравнению с 2022 годом и составил 15,8 млрд рублей. Это связано с рядом факторов, таких как широкое распространение онлайн-банкинга и мобильных платежных систем; уязвимость программного обеспечения и технических средств банков; недостаточная осведомленность клиентов о мерах безопасности; анонимность и трансграничный характер киберпространства, а также использование новых технологий, таких как искусственный интеллект, для проведения атак.

Несмотря на предпринимаемые меры по противодействию киберпреступности, данная проблема остается крайне актуальной. Действующее уголовное законодательство Российской Федерации не в полной мере отвечает современным вызовам, связанным с киберпреступностью в банковской сфере [7]. Существуют пробелы в правовом регулировании, а также трудности в квалификации отдельных видов киберпреступлений. Правоприменительная практика также сталкивается с рядом проблем, обусловленных сложностью доказывания вины, необходимостью специальных познаний в области информационных технологий, а также трансграничным характером многих киберпреступлений.

Основные положения работы

Предметом настоящего исследования являются уголовно-правовые и криминологические аспекты киберпреступности в сфере банковской деятельности.

Цель исследования – комплексный анализ проблем квалификации и противодействия киберпреступлениям в банковской сфере, а также разработка научно обоснованных предложений по совершенствованию законодательства и правоприменительной практики.

Методологическую основу исследования составили общенаучные (диалектический анализ, синтез, индукция, дедукция) и частнонаучные (формально-юридический, сравнительно-правовой, системно-структурный, статистический) методы познания.

Эмпирическую базу исследования составили: данные официальной статистики МВД России и Судебного департамента при Верховном Суде РФ о состоянии киберпреступности в России; материалы опубликованной судебной практики по делам о киберпреступлениях в банковской сфере; результаты обобщения материалов уголовных дел, находящихся в производстве следственных органов; аналитические отчеты и обзоры, подготовленные ведущими компаниями в сфере информационной безопасности (Group-IB, Kaspersky, PositiveTechnologies).

Одним из наиболее распространенных видов киберпреступлений в банковской сфере являются хищения денежных средств, совершаемые с использованием электронных средств платежа (ст. 159.3, 159.6 УК РФ)[1]. К таким хищениям можно отнести [5]:

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.12.2024) // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.

– *фишинговые атаки.* Злоумышленники рассылают электронные письма или СМС-сообщения, маскируясь под официальные уведомления от банков или платежных систем. В этих сообщениях содержатся ссылки на поддельные сайты, где пользователей просят ввести свои логины, пароли, данные банковских карт или другую конфиденциальную информацию. Получив эти данные, преступники получают доступ к счетам жертв. Пример. Массовая рассылка писем якобы от имени Сбербанка с требованием «подтвердить данные» под угрозой блокировки карты;

– *использование вредоносного ПО*. Злоумышленники заражают компьютеры или мобильные устройства пользователей вредоносными программами (троянами, кейлоггерами, стилерами), которые перехватывают данные банковских карт, пароли и другую информацию, вводимую пользователем. Пример. Троян ZeuS, модификации которого до сих пор встречаются, специализировался на краже банковских данных;

– *скимминг.* Установка на банкоматы специальных устройств (скиммеров), которые считывают данные с магнитной полосы карты, а также скрытых камер, записывающих PIN-код;

– *атаки на системы дистанционного банковского обслуживания* (ДБО). Взлом личных кабинетов пользователей в системах онлайн-банкинга с использованием украденных учетных данных или уязвимостей в программном обеспечении;

– *социальная инженерия*. Манипулирование сотрудниками банков или клиентами с целью получения доступа к информации или совершения несанкционированных операций. Пример. Звонок якобы от «службы безопасности банка» с просьбой сообщить код из СМС-сообщения для «отмены подозрительной операции».

Квалификация данных деяний вызывает ряд сложностей, связанных с определением предмета хищения, момента окончания преступления, а также разграничением смежных составов преступлений.

В доктрине уголовного права отсутствует единое мнение относительно предмета хищения при совершении преступлений, предусмотренных ст.ст. 159.3 и 159.6 УК РФ. Некоторые авторы полагают, что предметом хищения являются безналичные денежные средства [2, с. 90]. Другие же считают, что предметом хищения являются электронные денежные средства [4, с. 199]. Третьи указывают на то, что предметом хищения является право на имущество (право требования к банку) [1, с. 87]. Четвертая позиция, которая также заслуживает внимания, заключается в том, что предметом хищения может быть и информация (например, данные банковской карты), позволяющая получить доступ к денежным средствам.

Представляется, что наиболее обоснованной является позиция, согласно которой предметом хищения при совершении преступлений, предусмотренных ст.ст. 159.3 и 159.6 УК РФ, являются безналичные денежные средства, поскольку именно они находятся на счетах в банках и иных кредитных организациях, и именно они переходят в распоряжение виновного в результате совершения преступления. Электронные денежные средства, в свою очередь, являются лишь формой представления безналичных денежных средств. Однако учитывая развитие технологий и появ-

ление новых форм платежей (например, криптовалют), вопрос о предмете хищения в данной сфере остается дискуссионным и требует дальнейшего изучения.

Сложности возникают и при определении момента окончания хищения, совершенного с использованием электронных средств платежа. Пленум Верховного Суда РФ в своем Постановлении от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»[2] разъяснил, что хищение безналичных денежных средств считается оконченным с момента изъятия денежных средств с банковского счета владельца или электронных денежных средств, в результате которого владельцу этих средств причинен ущерб. Однако данное разъяснение не решает всех проблем. В частности, неясно, как квалифицировать действия лица, которое получило доступ к чужому банковскому счету, но не успело распорядиться денежными средствами (например, в результате блокировки счета банком или срабатывания систем фрод-мониторинга). Также остается открытым вопрос о квалификации действий, когда денежные средства были переведены на подконтрольный злоумышленнику счет, но еще не обналичены.

Представляется, что в таких случаях действия лица следует квалифицировать как покушение на хищение (ч. 3 ст. 30, ст. 159.3 или 159.6 УК РФ), поскольку умысел лица был направлен на завладение чужими денежными средствами, но преступление не было доведено до конца по не зависящим от него обстоятельствам.

Серьезную угрозу для банковской сферы представляют атаки на объекты критической информационной инфраструктуры (КИИ) банков (ст. 274.1 УК РФ). Данные атаки могут привести к нарушению работы банковских систем, утечке конфиденциальной информации, а также к значительным финансовым потерям. Такие атаки могут быть направлены: на системы процессинга платежей; автоматизированные банковские системы (АБС); системы межбанковских расчетов; сетевое оборудование; центры обработки данных (ЦОД) банков. Новейшей тенденцией являются атаки на цепочки поставок программного обеспечения, используемого банками, что позволяет злоумышленникам получить доступ к КИИ через уязвимости в сторонних компонентах. Примером может служить атака на компанию SolarWinds Inc. (США) в 2020 году, в результате которой пострадали многие организации, в том числе и финансовые.

Квалификация преступлений, предусмотренных ст. 274.1 УК РФ, также вызывает определенные трудности. В частности, не до конца ясен предмет данного преступления. В законе используется термин «критическая информационная инфраструктура», однако четкое определение данного понятия отсутствует. Это приводит к тому, что правоохранительные органы и суды могут по-разному толковать, какие именно объекты относятся к КИИ, и, соответственно, применять или не применять ст. 274.1 УК РФ. Это создает неопределенность в правоприменительной практике и затрудняет привлечение виновных лиц к ответственности.

[2] О судебной практике по делам о мошенничестве, присвоении и растрате : Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 // Бюллетень Верховного Суда РФ. – 2018. – № 1.

В Федеральном законе от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [3] дается определение КИИ, однако оно является достаточно общим и не позволяет однозначно определить, относится ли тот или иной объект к КИИ. В законе указано, что к КИИ относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергетики, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. Однако конкретного перечня объектов КИИ в банковской сфере в законе нет.

Представляется, что для решения данной проблемы необходимо разработать и утвердить перечень объектов КИИ в банковской сфере, а также установить четкие критерии отнесения объектов к КИИ. Этот перечень должен быть достаточно подробным и включать в себя, например, системы процессинга платежей, АБС, системы межбанковских расчетов, сетевое оборудование, ЦОД. Критерии отнесения объектов к КИИ должны учитывать такие факторы, как значимость объекта для обеспечения функционирования банковской системы, потенциальный ущерб от нарушения его работы, наличие подключений к другим объектам КИИ.

Еще одной проблемой является квалификация неправомерного доступа к банковской тайне (ст. 183 УК РФ). В условиях цифровизации банковской деятельности и широкого использования электронных каналов коммуникации риски неправомерного доступа к банковской тайне значительно возрастают. Такой доступ может быть осуществлен как извне (например, хакерами), так и изнутри (например, недобросовестными сотрудниками банка).

В доктрине уголовного права и в правоприменительной практике нет единого мнения о том, что следует понимать под «незаконными способами» получения сведений, составляющих банковскую тайну. Некоторые авторы полагают, что к незаконным способам следует относить любые действия, совершенные в нарушение установленного законом порядка получения таких сведений [3, с. 63]. Другие же считают, что к незаконным способам следует относить только те действия, которые прямо запрещены законом [6, с. 339]. Третья точка зрения состоит в том, что незаконными следует считать не только прямо запрещенные законом действия, но и действия, совершенные с нарушением этических норм и правил делового оборота.

Представляется, что более правильным является первый подход, поскольку он обеспечивает более полную защиту банковской тайны. При этом необходимо учитывать, что способы получения сведений могут быть самыми разнообразными: от использования вредоносного ПО до подкупа сотрудников банка.

[3] О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ // Собрание законодательства РФ. – 2017. – № 31 (Часть I). – Ст. 4736.

Кроме того, необходимо уточнить понятие «банковская тайна», включив в него не только сведения о счетах и операциях клиентов, но и иную конфиденциальную информацию, относящуюся к деятельности банков (например, информацию о системах безопасности, программном обеспечении, алгоритмах шифрования, внутренних регламентах и т.д.). Это связано с тем, что утечка такой информации может нанести банку не меньший ущерб, чем раскрытие сведений о счетах клиентов.

Важным направлением противодействия киберпреступности в банковской сфере является международное сотрудничество. Киберпреступность, как правило, носит трансграничный характер, поэтому эффективная борьба с ней невозможна без тесного взаимодействия правоохранительных органов разных стран. Это взаимодействие может осуществляться в рамках международных организаций (Интерпол, Европол), а также на основе двусторонних и многосторонних соглашений.

Россия активно участвует в международном сотрудничестве в сфере борьбы с киберпреступностью, являясь участником ряда международных договоров и соглашений (например, Конвенции Совета Европы о киберпреступности 2001 г.)[4]. Однако существующий уровень международного сотрудничества не всегда отвечает потребностям борьбы с киберпреступностью в банковской сфере. Проблемами международного сотрудничества являются различия в законодательстве разных стран, сложности с установлением юрисдикции, длительные сроки исполнения запросов о правовой помощи.

Помимо международного сотрудничества, полезно изучать и зарубежный опыт борьбы с киберпреступностью. Например, в США действует Закон о компьютерном мошенничестве и злоупотреблениях (Computer Fraud and Abuse Act, CFAA), который устанавливает уголовную ответственность за широкий спектр киберпреступлений. В Европейском союзе действует Директива о сетевой и информационной безопасности (NIS Directive), которая обязывает государства-члены принимать меры по обеспечению кибербезопасности критической инфраструктуры, включая банковский сектор. Также интерес представляет опыт Китая, где создана развитая система контроля за интернет-пространством и активно применяются технологии искусственного интеллекта для выявления киберпреступлений.

Необходимо активизировать взаимодействие с зарубежными партнерами по вопросам обмена информацией о киберпреступлениях, проведения совместных расследований, выдачи преступников, а также оказания взаимной правовой помощи. Одним из перспективных направлений является создание международных центров по борьбе с киберпреступностью, где могли бы работать специалисты из разных стран.

Для повышения уровня кибербезопасности банкам рекомендуется:

– регулярно проводить аудит информационной безопасности и тестирование на проникновение (penetration testing). Это позволяет выявлять

[4] Конвенция о киберпреступности (ETS № 185) (Будапешт, 23 ноября 2001 г.) // Собрание законодательства РФ. – 2006. – № 31. – Ст. 3552.

уязвимости в системах защиты банка и своевременно принимать меры по их устранению;

– внедрять многофакторную аутентификацию (MFA) для доступа к онлайн-банкингу и другим критически важным системам. MFA предполагает использование нескольких факторов аутентификации (например, пароль и код из СМС-сообщения), что значительно затрудняет несанкционированный доступ;

– обучать сотрудников правилам кибербезопасности и проводить тренировки по распознаванию фишинговых атак. Сотрудники банка должны знать основные виды киберугроз и уметь распознавать подозрительные письма, сообщения и звонки;

– использовать современные средства защиты от вредоносного программного обеспечения и DDoS-атак. Это включает в себя антивирусное ПО, межсетевые экраны, системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS);

– разработать план реагирования на инциденты информационной безопасности и регулярно проводить его тестирование. План должен определять порядок действий сотрудников банка в случае кибератаки, а также предусматривать меры по минимизации ущерба и восстановлению работы систем;

– внедрить систему фрод-мониторинга, которая в режиме реального времени анализирует транзакции на предмет подозрительной активности и блокирует их при необходимости;

– регулярно обновлять программное обеспечение и операционные системы для устранения известных уязвимостей;

– вводить резервное копирование данных и создавать резервные копии систем для обеспечения возможности восстановления в случае сбоя.

Заключение

Проведенное исследование позволяет сделать следующие выводы:

1) киберпреступность в сфере банковской деятельности представляет собой сложный и динамично развивающийся вид преступности, требующий постоянного совершенствования мер противодействия;

2) действующее уголовное законодательство Российской Федерации не в полной мере отвечает современным вызовам, связанным с киберпреступностью в банковской сфере. Существуют пробелы в правовом регулировании, а также трудности в квалификации отдельных видов киберпреступлений;

3) для повышения эффективности борьбы с киберпреступностью в банковской сфере необходимо:

– уточнить понятие «критическая информационная инфраструктура» в ст. 274.1 УК РФ и разработать перечень объектов КИИ в банковской сфере;

– конкретизировать понятие «незаконные способы» получения сведений, составляющих банковскую тайну, в ст. 183 УК РФ. Расширить перечень сведений, составляющих банковскую тайну;

– усилить уголовную ответственность за хищения, совершаемые с использованием электронных средств платежа, путем внесения изменений в ст.ст. 159.3 и 159.6 УК РФ;

– активизировать международное сотрудничество в сфере борьбы с киберпреступностью в банковской сфере, изучать и адаптировать передовой зарубежный опыт;

– повысить уровень подготовки специалистов, занимающихся раскрытием, расследованием киберпреступлений, а также рассмотрением их в суде.

– банкам следует принимать активные меры по повышению собственного уровня кибербезопасности.

Реализация предложенных мер позволит повысить эффективность борьбы с киберпреступностью в банковской сфере, обеспечить защиту прав и законных интересов граждан и организаций, а также укрепить финансовую стабильность государства. Дальнейшие исследования данной проблематики должны быть направлены на изучение новых видов киберпреступлений в банковской сфере, а также на разработку новых методов и средств противодействия им.

Список литературы

1. Безверхов, А. Г. Имущественные преступления / А. Г. Безверхов. – Самара : Изд-во Самар. гос. ун-та, 2022. – 368 с.

2. Буянова, А. О. Уголовно-правовая характеристика преступлений, связанных с хищением чужого имущества, совершенных с использованием информационно-коммуникационных технологий / А. О. Буянова // Молодой ученый. – 2022. – № 41(436). – С. 88 – 91.

3. Вехов, В. Б. Компьютерные преступления: способы совершения и раскрытия / В. Б. Вехов ; под ред. Б. П. Смагоринского. – Москва : Право и закон, 2021. – 182 с.

4. Егоров, В. С. Проблемы квалификации преступлений, связанных с хищением безналичных и электронных денежных средств / В. С. Егоров, А. Н. Порошина // Молодой ученый. – 2020. – № 50(340). – С. 199 – 200.

5. Зайнулабидов, М. З. Киберпреступления в кредитно-финансовой сфере / М. З. Зайнулабидов, О. В. Исаев, О. В. Толстых // Закон и право. – 2024. – № 8. – С. 68 – 73. doi: 10.24412/2073-3313-2024-8-68-73

6. Караваев, Н. А. Неправомерный доступ к компьютерной информации: проблемы квалификации / Н. А. Караваев // Молодой ученый. – 2023. – № 23(470). – С. 338 – 340.

7. Тропина, Т. Л. Киберпреступность: понятие, состояние, проблемы уголовно-правовой борьбы / Т. Л. Тропина // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2022. – № 1. – С. 105 – 115.

References

1. Bezverkhov A.G. *Imushchestvennyye prestupleniya* [Property Crimes], Samara: Izdatel’stvo Samar. gos. un-ta, 2022, 368 p. (In Russ.).

2. Buyanova A.O. [Criminal-legal characteristics of crimes related to the theft of someone else's property, committed using information and communication technologies], *Molodoy uchenyy* [Young Scientist], 2022, no. 41(436), pp. 88-91. (In Russ., abstract in Eng.).

3. Vekhov V.B., Smagorinsky B.P. (Ed.). *Komp'yuternyye prestupleniya: sposoby sovershеniya i raskrytiya* [Computer Crimes: Methods of Commission and Detection], Moscow: Pravo i zakon, 2021, 182 p. (In Russ.).

4. Yegorov V.S., Poroshina A.N. [Problems of qualification of crimes related to the theft of non-cash and electronic money], *Molodoy uchenyy* [Young Scientist], 2020, no. 50(340), pp. 199-200. (In Russ., abstract in Eng.).

5. Zaynulabidov M.Z., Isayev O.V., Tolstykh O.V. [Cybercrimes in the credit and financial sphere], *Zakon i pravo* [Law and Order], 2024, no. 8, pp. 68-73. doi: 10.24412/2073-3313-2024-8-68-73 (In Russ., abstract in Eng.).

6. Karavayev N.A. [Unauthorized access to computer information: problems of qualification], *Molodoy uchenyy* [Young Scientist], 2023, no. 23(470), pp. 338-340. (In Russ., abstract in Eng.).

7. Tropina T.L. [Cybercrime: Concept, Status, and Problems of Criminal-Legal Struggle], *Vestnik Universiteta imeni O. Ye. Kutafina (MGYUA)* [Bulletin of the Kutafin Moscow State Law University (MSAL)], 2022, no. 1, pp. 105-115. (In Russ., abstract in Eng.).

Cybercrime in the Banking Sector: Qualification and Counteraction Issues

H. A. Akkaeva, *Cand. Sci. (Law), Associate Professor, Google Deputy Head of the Department of Science and Innovation, Kabardino-Balkarian State Agricultural University named after V.M. Kokov, Nalchik, Kabardino-Balkarian Republic, Russia; akkaevah@mail.ru*

The article deals with a comprehensive analysis of the problems of qualification and counteraction to cybercrimes in the banking sector. The evolution of cybercrime, its specifics in the banking sector, as well as the shortcomings of the current criminal legislation of Russia in terms of regulating responsibility for these acts are considered. Particular attention is paid to the problems of qualification of embezzlement committed using electronic means of payment, attacks on critical information infrastructure of banks, as well as illegal access to banking secrecy. The paper analyzes various scientific approaches to solving these problems, and also suggests specific measures to improve legislation and law enforcement practice. The issues of international cooperation in the fight against cybercrime in the banking sector are investigated.

Keywords: cybercrime; banking; electronic means of payment; critical information infrastructure; banking secrecy; theft; unauthorized access; qualification of crimes; criminal liability; international cooperation.

Статья поступила в редакцию 08.10.2025

При цитировании использовать:

Аккаева Х. А. Киберпреступность в сфере банковской деятельности: квалификация и проблемы противодействия // Право: история и современность. – 2026. – Т. 10, № 1. – С. 099 – 107. doi: 10.17277/pravo.2026.01.pp.099-107