УДК 336.71

ОСНОВНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ЗАЩИТЫ ОТ ФИНАНСОВОГО МОШЕННИЧЕСТВА В БАНКОВСКОЙ СФЕРЕ
THE MAIN DIRECTIONS OF IMPROVING PROTECTION AGAINST FINANCIAL FRAUD IN THE BANKING SECTOR

[1]С.В. Пелькова, [1]Е.В. Мазикова, [2]Е.С. Соколова
[1]S.V. Pelkova, [1]E.V. Mazikova, [2]E.S. Sokolova

1. ФГАОУ ВО Тюменский государственный университет, Тюмень, email: svepelkova@yandex.ru

Tyumen State University, Tyumen, email: svepelkova@yandex.ru.

2. ФГБОУ ВО Государственный аграрный университет Северного Зауралья, Тюмень, emai: sok-evgenia@yandex.ru

The State Agrarian University of the Northern Trans-Urals, Tyumen, email: sok-evgenia@yandex.ru

Аннотация.
Актуальность темы заключается в том, что финансовые мошенничества в банковской сфере в России получили широкое распространение. Что подтверждается аналитической отчетностью, а также статистикой Центрального банка РФ и правоохранительных органов. Для повышения эффективности своей деятельности мошенники применяют методы и приемы социальной инженерии, адаптируют схемы к условиям объективной действительности, разрабатывают новые сценарии и обходят алгоритмы защитных систем банковских учреждений. Как следствие, для предотвращения финансовых мошенничеств в банковской сфере необходимостью будет являться планомерное совершенствование соответствующей деятельности, так как данные статистики свидетельствуют о том, что на современном этапе развития она не является совершенной.

Annotation.
The relevance of the topic lies in the fact that financial fraud in the banking sector in Russia has become widespread. This is confirmed by statistical, analytical reports, as well as statistics of law enforcement agencies. To increase the efficiency of their activities, fraudsters use methods and techniques of social engineering, adapt schemes to the conditions of objective reality, develop new scenarios and bypass algorithms of protective systems of banking institutions. As a consequence, in order to prevent financial fraud in the banking sector, it will be necessary to systematically improve the relevant activities, since statistical data indicate that at the present stage of development it is not perfect.

Ключевые слова: банковская сфера, финансовые мошенничества, социальная инженерия.

Keywords: banking, financial fraud, social engineering.

Введение.

Финансовое мошенничество в банковской сфере – это хищение денег или имущества, приобретение права на имущество при помощи обмана или злоупотребления доверием. Обман предусматривает сознательное введение потерпевшего в заблуждение. Такая трактовка предусмотрена в ст.159 УК РФ.

Цель исследования.

Определение основных направлений совершенствования защиты от финансового мошенничества в банковской сфере в РФ на основе комплексного анализа.

Объекты и методы исследования.

Объектом исследования являются финансовые мошенничества в банковской сфере России.

Методы исследования: формально – логический, структурно - функциональный, метод сравнительных исследований и другие методы научного познания.

Результаты и их обсуждение.

Операции в банковской сфере носят разносторонний и обширный характер, что позволяет совершать финансовые мошенничества различными способами. Анализ общественно опасных деяний позволяет классифицировать их на виды в зависимости от того, какой способ мошеннических действий применялся в том или ином случае [5] По данному критерию выделяют несколько видов мошенничества, представленных на рис. 1.

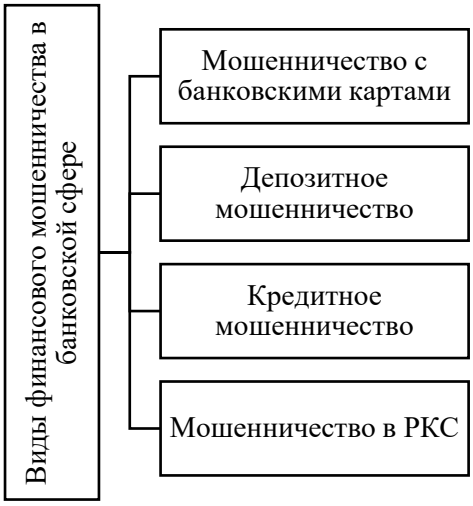

Рис.1 Виды финансового мошенничества в банковской сфере

По официальным данным Центрального банка РФ в 2022г. было зафиксировано более 877 тыс. случаев хищения денежных средств с банковских счетов. В 2021г. этот показатель был выше на 15,3 % (рис.2). Статистика хищений денежных средств со счетов клиентов в 2022г. сократилась по сравнению с предыдущим периодом, при этом сумма ущерба от всех действий, совершенных мошенниками в 2022г. увеличилась на 4%. Согласно официальным данным, большая часть ущерба нанесена при работе дистанционного банковского обслуживания.

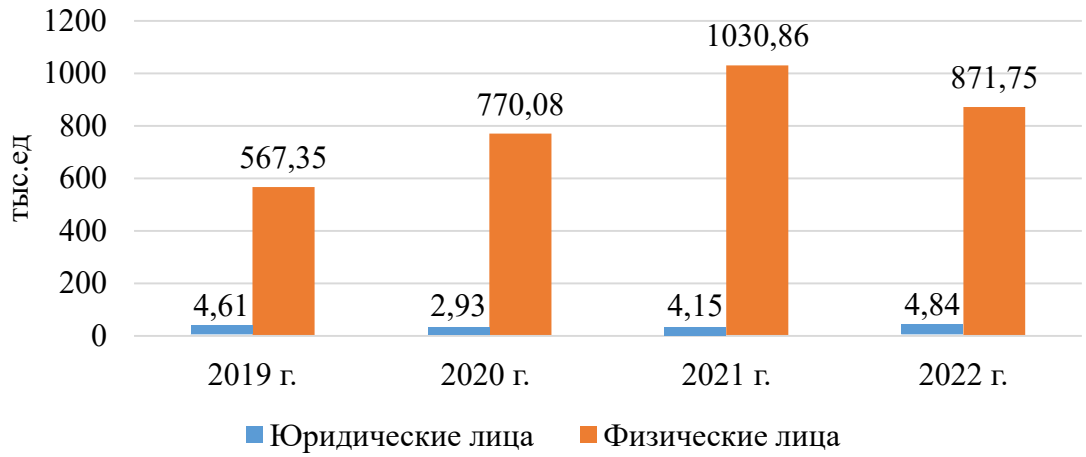

Рис.2 Динамика количества хищений денежных средств с банковских счетов, тыс. ед.

* Источник: Годовой отчет Банка России

Наибольшая часть операций, совершенных без согласия клиентов, связана с оплатой услуг и товаров в сети «Интернет». При этом, весьма существенная часть приходится на мошенничества, совершенные с помощью дистанционных сервисов: онлайн-банки. По официальной статистике аналитической отчетности регулятора, после получения доступа к данным сервисам, мошенники приобретают возможность совершить сразу несколько эпизодов мошенничества, таких как: похищение всей суммы денежных средств со счета клиента, оформление кредита на потенциального клиента. Наименьший объем мошенничеств приходится на кражу денежных средств при использовании карт без согласия их владельца в терминалах и банкоматах.

Банковские учреждения в 2022г. осуществили возврат на 4,4 % от общего объема краж, что составило 618,4 млн. руб., в 2021г. соответствующие показатели составили 6,8 % (920,5 млн. руб.), а в 2020г. – 11,3 %, что составило более 1 млрд. руб. При этом доля возмещенных денежных средств снижается, обусловлено это тем, что мошеннические схемы сегодня планомерно совершенствуются и клиенту весьма затруднительно доказать, что денежные средства были сняты или переведены не им, а третьим лицом. Все вышеперечисленное позволяет сделать вывод о важности принятия превентивных мер, равно как тех мер, которые были бы направлены на совершенствование механизма защиты от финансовых мошенничеств в банковской сфере. Стоит отметить, что хищения с использованием методов и средств социальной инженерии составили в 2022г. - 50,4 % от всех случаев финансового мошенничества, что выше показателя 2021г. - 49,4 %.

В денежном выражении одна операция, совершенная без согласия клиента, при случаях финансового мошенничества, составляет 15,32 тыс. руб. для физических лиц и 166,91 тыс. руб. для юридических лиц. Количество операций, совершенных без согласия клиентов, отражено на рис. 3.

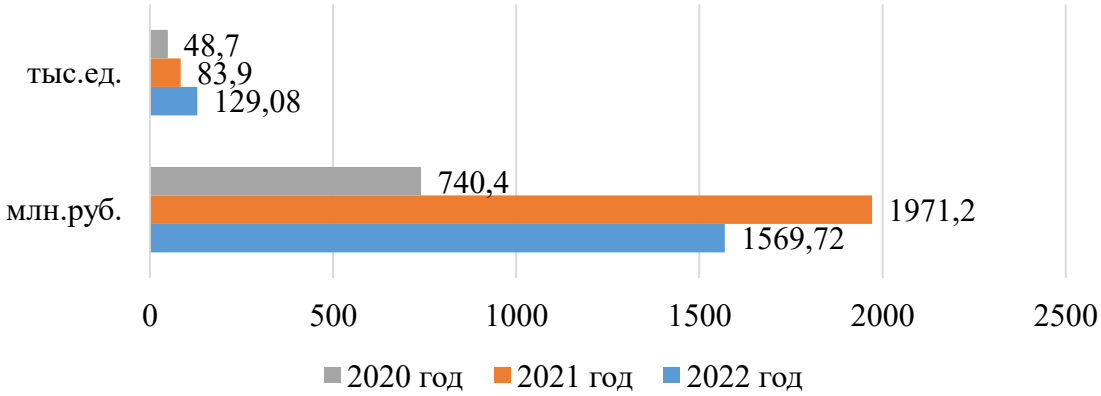

Рис.3 Количество и объем операций, совершенных без согласия клиентов в банкоматах, терминалах и импортерах

* Источник: Годовой отчет Банка России

Количество операций без согласия клиентов в терминалах и банкоматах в 2022г. возросло за анализируемый период, однако сумма похищенных денежных средств уменьшилась по сравнению с предыдущим годом.

Субъектный состав мошенничества в банковской сфере распределяется различным образом (рис.4).

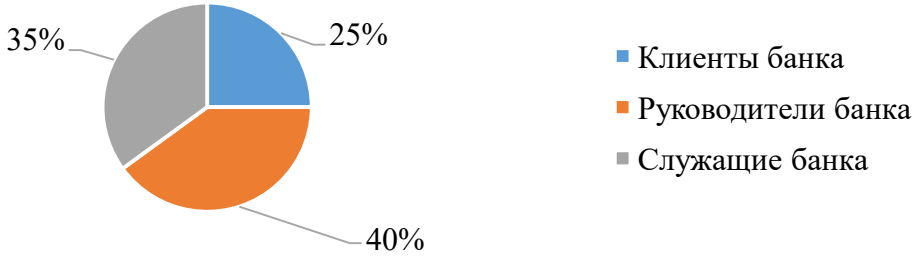

Рис.4 Структура субъектов, совершающих финансовые мошенничества в банковской сфере РФ, %

* Источник: Годовой отчет Банка России

Наибольшее количество финансовых мошенничеств совершается непосредственно руководителями, так как они имеют доступ к персональной и финансовой информации. 35 % данных преступлений совершается служащими банка, которые также имеют доступ к персональным и финансовым данным клиентов и могут совершать тот или иной вид финансового мошенничества, например, расчетно-кассовое, кредитное или депозитное мошенничество. 25 % мошенничеств совершают клиенты, которые подделывают документы, предоставляют заведомо ложную информацию или совершают иные действия. В данный процент входят как рядовые граждане, так и профессиональные мошенники. Каналы финансового мошенничества в 2022г. распределились следующим образом (рис.5):

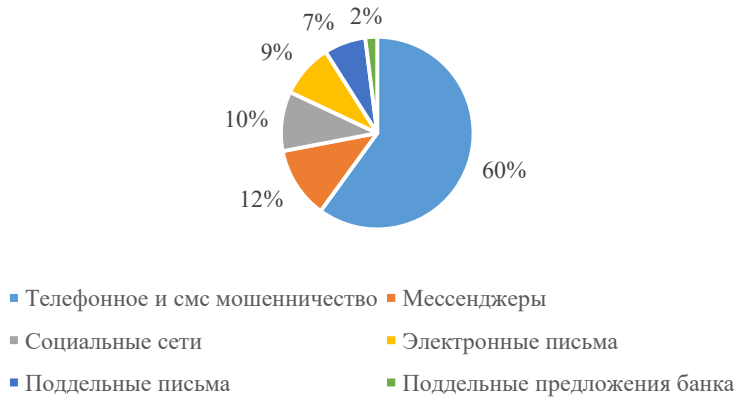

Рис.5 Структура источников финансового мошенничества в банковской сфере РФ за 2022г., %

* Источник: Годовой отчет Банка России

Телефонное и смс-мошенничество лидирует, в связи с чем предусматривается необходимость в принятии широкой совокупности превентивных мер, направленных на недопущение этих преступных деяний.

Одной из таких мер может служить внедрение комбинированных систем фрод-мониторинга, которые выступают в качестве эффективного стандарта системы, так как они построены на правилах, алгоритмах и списках, а также моделях Al, нескольких уровнях проверки и комбинации этих инструментов и позволяют выявить даже сложные признаки мошенничества. Комбинированные модели фрод-мониторинга - это такие антифрод-системы, которые выполняют широкую совокупность функций: проверяют транзакции в режиме реального времени, создают графовые модели поведения мошенников и клиентов, анализируют гео-локации, классифицируют жалобы клиентов, выделяя случаи ошибочного отклонений операций, проводят скоринг. На рис. 6 отражены этапы системы противодействия мошенничества онлайн-контура фрод-мониторинга.

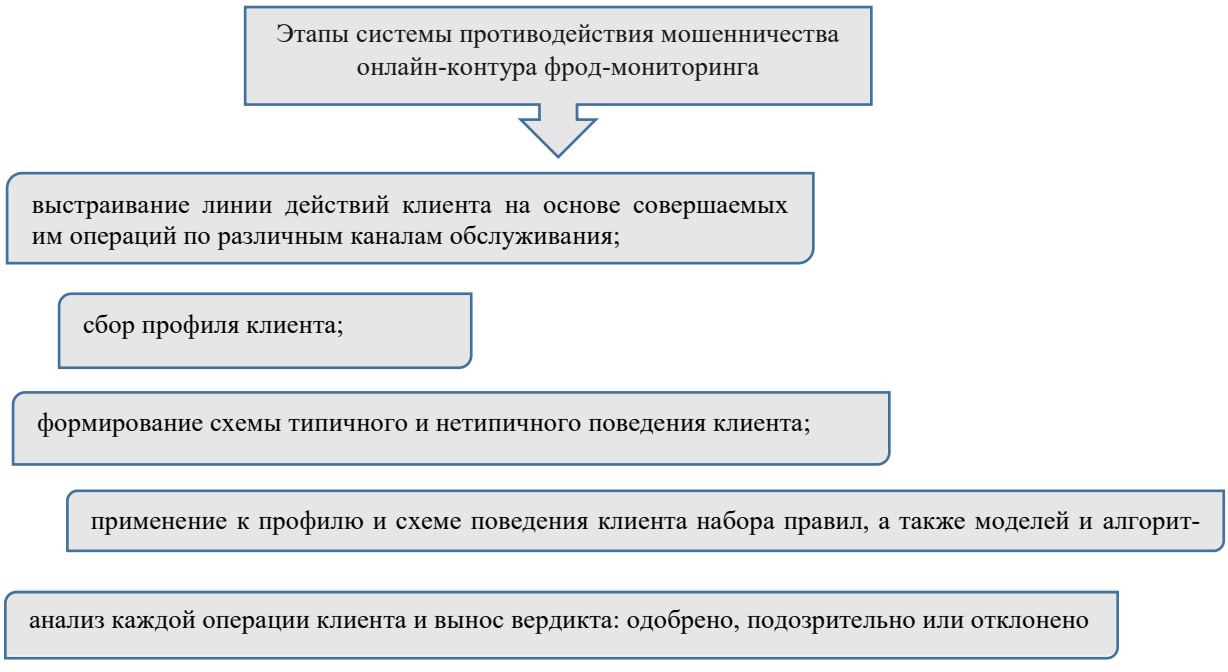

Рис.6 Этапы системы противодействия мошенничества онлайн-контура фрод-мониторинга

Также на фоне того, что операций, совершаемых клиентами, больше, чем операций, совершаемых без их согласия, присутствует несбалансированность распределения данных на классы. Способом избегания данной проблемы может служить применение обучения антифрод-системы с помощью использования сети CycleGAN, применяемая в целях генерации синтетических операций мошенников. По мере использования дроп-счетов, система выявит операции с высокой степенью вероятности. В случае определения такой операции перевод на дроп-счет, будет приостанавливаться в соответствии со ст. 9 ФЗ от 27.06.2011 г. № 161-ФЗ «О национальной платежной системе». Переводы на дроп-счета классифицируются на два вида: когда перевод осуществляет непосредственно-мошенник и когда его делает сам клиент, но под руководством мошенника. На этом фоне, первый тип операции будет блокироваться сразу, а при втором типе перед банковским учреждением стоит задача дозвониться для клиента и убедить не переводить на данный счет денежные средства. Одновременно с этим, данный механизм едва ли является совершенным, в том случае, если клиент добросовестный и настаивает на исполнении операции, банковская организация не имеет прав не исполнить ее, причем даже в том случае, если в ней усматриваются признаки мошенничества в отношении клиента.

Таким образом, в практику деятельности кредитных учреждений стоит внедрять системы фрод-мониторинга комбинированного типа с обучением по сети CycleGAN [8]. Схема работы системы в данной вариации представлена на рис. 7.

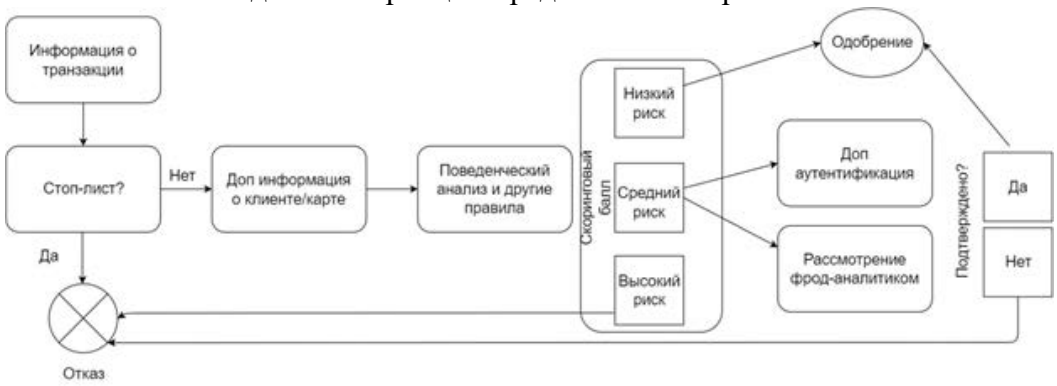

Рис.7 Схема работы предлагаемой для внедрения системы фрод-мониторинга

При исполнении данной схемы каждая операция подлежит обязательному этапу оценки – скорингу. Легитимным операциям будет присваивается значение от 0 до 500, подозрительным от 501 до 999, отклоняемым операциям - 1000 и выше. При этом, профиль клиента, который подлежит анализу, включает в себя ID, логин, номер мобильного телефона, приложение на компьютере и мобильное приложение, с помощью которого клиент входит в онлайн-банк. Кроме этого, в указанный профиль включаются типы и набор операций, которыми клиент пользуется, место его расположения, а также наиболее типичные локации. В данном случае, оценка риска будет позиционироваться в виде модели в которую передаются данные профиля клиента, и данные об операции, совершаемой в текущий момент. Далее возможны три варианта исхода событий: 1)

финансовая организация передает операцию в дальнейшую обработку, 2) финансовая организация требует дополнительного подтверждения от клиента на проведение операции, 3) операция отклоняется финансовой организацией. В основу фрод-анализа закладывают и риск-ориентированную аутентификацию (RBA), подразумевающую выбор того или иного метода аутентификации в зависимости от уровня риска операции. В процессе подтверждения определенного типа операции выбирается один или несколько способов: биометрия, паспортные данные или звонок с контактного центра. На фоне того, что данная система проводит проверку более чем по 150 параметрам, RBA рекомендована для внедрения в систему форд-мониторинга. Так, именно с помощью RBA есть возможность проанализировать локацию, тип устройства, время суток, новизну или привычность операции и иные критерии. Если будет выявлено отклонение, проводится сопоставление веса данного отклонения с количество пунктов этих отклонений. Затем присваивается уровень риска и фактор подтверждения: IVR – звонок автоматизированной системы, SMS-сообщение с кодом, RUSH, QR-код, карта + пин-код и иные формы (вместе или в совокупности). Отметим, что разные факторы RBA требуют разного применения, например, если клиент на самостоятельной основе переводит денежные средства по звонку мошенника через банкомат, использование биометрии нецелесообразно, так как в данном случае это не позволит отклонить мошенническую операцию, которая будет в системе подтверждена. Как следствие, в данном случае наиболее оптимален звонок от сотрудника банка.

В завершении анализа фрод-мониторинга, как варианта для эффективного предотвращения финансового мошенничества в банковской сфере отметим, что данная система применима не только для внешнего мошенничества, но и для защиты от внутреннего мошенничества, необходимость в который выявлена в данном исследовании ранее. Более того, указанная система применима в целях борьбы с DDoS-атаками. Данная система способна выявить аномалии по всем операциям, произвести блокировку выявленных операций и не допущения их в процессинг. Как следствие, система форд-мониторинга применима для всех разновидностей финансового мошенничества, что актуализирует ее применение на практике.

Такие системы основаны на использовании моделей искусственного интеллекта, равно как статистических правилах, алгоритмах и списках, в связи с чем, показывают высокую эффективность. Проведенный анализ позволил выявить все параметры такой системы, при которых ее применение будет наиболее эффективным.

Также эффективным инструментом для предотвращения мошенничества в банковской сфере и снижения рисков такового является «форензик», который также стоит внедрять в практику всех отечественных кредитных организаций. Форензик (forensic) предусматривает всестороннее, независимое расследование, которое проводят незаинтересованные лица и направленное на выявление и на предотвращение различных противоправных действий в отношении кредитных учреждений и возвращение активов, которые были из них выведены. Указанное расследование вполне может выявить и мошенничество в банковской сфере, но несмотря на свою эффективность, форензик в России не получил достаточного распространения. Полагаем, что во многом это обусловлено тем, что средняя стоимость форензик-расследования составляет 10-15 млн. рублей для крупного банка, 7-10 млн. руб. для среднего банка и 3-6 млн. руб. для мелкого банка. На этом фоне, многие кредитные учреждения не прибегают к услугам подобного рода, однако они не учитывают, что потери, которые они могут понести из-за

своевременно не предотвращенных действий мошенников, намного выше. Как следствие, такие расследования должны войти в практику банков, учитывая, что они проводятся широкой совокупностью специалистов: юристами, а также аудиторами, IT-специалистами, оценщиками. Более того, на территории нашей страны действуют крупные игроки этого рынка, в частности, консалтинговые компании, входящие в «большую четверку» (Deloitte, EY, PwC, KPMG).

В 2021 г. в РФ был создан Forensic Alliance, суть деятельности данного объединения состоит в партнерстве разных независимых экспертов, которые проводят форензик-расследования для выявления, равно как предотвращения финансовых мошенничеств в банковской сфере. Полагаем, что низкая популярность форензик-расследований также обусловлена тем, что законодательством РФ не установлено требование к обязательному проведению таких расследований, однако проведенный анализ показал, что объективной необходимостью является самостоятельная организация банками проведения таковых, так как это позволит оптимизировать деятельность по пресечению и профилактике финансовых мошенничеств. Очевидно, что прибегать к данной услуге целесообразно не только для расследования фактов злоупотреблений, что наблюдается на современном этапе развития, но и для их предупреждения, однако пока этого не наблюдается [7].

Кроме предложенных инструментов, ограничить последствия финансового мошенничества возможно с помощью внутреннего аудитора. Не редко при фальсификации финансовой отчетности допускаются некоторые виды искажения отчетности. Эти действия образуют внутреннее мошенничество в кредитной организации, обнаружить которые способен внутренний аудитор. На этом фоне также необходимо указать на то, что банковским организациям необходимо регулировать и повышать качество своей внутренней политики: проводить более активную работу по оценке рисков и сбору данных, проводить обучение персонала, в том числе, для ознакомления с новыми схемами мошеннических действий [6].

Заключение.

Таким образом, деятельность по предотвращению различных финансовых мошенничеств в банковской сфере нуждается в совершенствовании. Выявлено, что его осуществление представляется возможным после проведения широкой совокупности мероприятий, состоящих в изменении и дополнении нормативно-правовых актов, внедрении цифровых технологий, улучшении взаимодействия между ведомствами, проведении форензик-расследовании и использования «антифрод-систем».

Список литературы

1. Виды мошенничества. [Электронный ресурс]. URL: https://www.banki.ru/wikibank/vidyi_moshennichestva (дата обращения: 15.11.2023).
2. Годовой отчет Банка России 2022. [Электронный ресурс].URL: https://www.cbr.ru/Collection/Collection/File/43872/ar_2022.pdf (дата обращения: 09.11.2023)/
3. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996, № 14-ФЗ: ред. от 01.07.2021: принят Государственной Думой 22 декабря 1995 года. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 01.11.2023).

4. Истории о мошенничестве. [Электронный ресурс]. URL: https://fincult.info/rake/?tags=1524 (дата обращения: 09.11.2023).
5. Капинус О.С. Комментарий к Уголовному кодексу Российской Федерации: научно-практический комментарий / под ред. О.С. Капинус. М.: Проспект, 2019. 1376 с.
6. Карпович О.Г. Актуальные уголовно-правовые проблемы борьбы с финансовым мошенничеством: монография. М.: ЮНИТИ-ДАНА, 2017. 271 с.
7. Кузнецова Е.Г. Обман как способ хищения при мошенничестве // Вестник Уральского института экономики, управления и права. 2017. № 3. С. 40-45.
8. Ларионова С.Л. Организация работы по борьбе с мошенничеством в кредитной организации // Вопросы безопасности. 2022. № 4. С. 15-26.
9. Обзор операций, совершенных без согласия клиентов финансовых организаций / Отчет Банка России. [Электронный ресурс]. URL: https://cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 09.11.2023).