Студенческий научный электронный журнал
StudArctic Forum

ПЕТРОЗАВОДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Т. 8, № 1. С. 83—90 **Экономика** **2023**

Научная статья
УДК 343.72

БОГДАНОВ
Артём Андреевич

бакалавриат, Северный институт Всероссийского государственного университета юстиции (Петрозаводск, Российская Федерация)
9637421111@mail.ru

ПРОФИЛАКТИКА И ПРЕДУПРЕЖДЕНИЕ ФИНАНСОВОГО МОШЕННИЧЕСТВА В СОВРЕМЕННОЙ РОССИИ

Научный руководитель:
Левкин Николай Владимирович
Статья поступила: 30.03.2023;
Принята к публикации: 31.03.2023;
Опубликована: 15.04.2023

Аннотация. Цель статьи - дать всеобъемлющий обзор финансового мошенничества, которое включает финансовые преступления и кибермошенничество. В работе освещаются потенциальные жертвы финансового мошенничества, виды кибермошенничества, технологии, используемые мошенниками.

Ключевые слова: финансовое мошенничество, финансовые преступления, кибермошенничество, кибербезопасность, мошенники

Для цитирования: Богданов А. А. Профилактика и предупреждение финансового мошенничества в современной России // StudArctic Forum. 2023. Т. 8, № 1. С. 83—90.

Финансовое мошенничество – это один из наиболее распространенных видов преступлений в России. Финансовое мошенничество становится все более серьезной проблемой для финансового права в современном мире, поскольку финансовые преступления и кибермошенничество представляют значительные угрозы как для отдельных лиц, так и для организаций. В последние годы органы государственной власти предприняли усилия по борьбе с этими преступлениями и укреплению правовых механизмов и систем кибербезопасности для защиты от них. Однако распространенность финансового мошенничества остается серьезной проблемой, и очевидно, что для решения этой проблемы необходимы дальнейшие усилия.

Финансовое мошенничество может принимать множество различных форм, включая растрату, отмывание денег, финансовые пирамиды и кибермошенничество. Эти преступления могут иметь серьезные финансовые и личные последствия для жертв, включая финансовые потери, ущерб репутации и эмоциональные расстройства.

Кибермошенничество стало особенно серьезной угрозой в последние годы, поскольку мошенники становятся все более изощренными в своих методах. Используя такие технологии, как фишинг, социальная инженерия и вредоносное ПО, киберпреступники могут получить доступ к конфиденциальной финансовой информации и украсть средства у частных лиц и организаций.

Для борьбы с финансовым мошенничеством законодатель в РФ применяет многогранный подход, включая ужесточение наказаний за финансовые преступления, введение новых правил и стандартов для финансовых учреждений и инвестиции в технологические решения для выявления и предотвращения мошенничества. Однако для решения этой сохраняющейся проблемы и защиты отдельных лиц и организаций от финансового мошенничества требуется дополнительная работа.

В этой статье мы рассмотрим различные виды финансового мошенничества, технологии, используемые мошенниками, и меры, принимаемые для борьбы с финансовым мошенничеством в России. Мы также изучим проблемы, которые остаются в этой области, и необходимость продолжения усилий по защите от финансового мошенничества в предстоящие годы.

ФИНАНСОВЫЕ ПРЕСТУПЛЕНИЯ В РОССИИ

Какие виды финансовых преступлений существуют в России

В России существует множество видов финансовых преступлений, в числе которых:

1. Незаконная банковская деятельность: в том числе создание фиктивных банков, мошенническое использование банковских карт и платежных систем, отмывание денег через банковские счета, обман заемщиков и вкладчиков.
2. Финансовое мошенничество: в том числе мошенничество с ценными бумагами, злоупотребление инсайдерской информацией, фальсификация финансовой отчетности, мошенничество в сфере страхования и пенсионного обеспечения.
3. Налоговые преступления: в том числе уклонение от уплаты налогов, подделка документов, фиктивное предпринимательство, сокрытие доходов и имущества.
4. Киберпреступления: в том числе мошенничество в сети интернет, взлом банковских систем и электронных кошельков, фишинг, скимминг, создание вирусов и троянов.
5. Отмывание денег: преступная деятельность по переводу денег, полученных незаконным путем, через различные банковские и финансовые схемы, с целью законного обналичивания.
6. Коррупция: в том числе получение взятки, дача взятки, злоупотребление должностными полномочиями, злоупотребление бюджетными средствами.

Все эти виды преступлений наносят серьезный ущерб экономике России, поэтому борьба с ними является одним из приоритетных направлений развития финансового права в стране.

Статистика финансовых преступлений в России

Данные RTM Group показывают, что в 2021 году количество киберпреступлений в России выросло на 1,4% по сравнению с предыдущим годом и в 1,8 раза по сравнению с 2019 годом. Согласно оценке, число заявлений о мошенничестве выросло на 5,1%, превысив 249 тысяч, а число заявлений о компьютерных преступлениях со взломом снизилось на 10,6%, до 157 тысяч. Около четверти преступлений были связаны с другими правонарушениями, включая незаконные азартные игры. Ущерб России от действий хакеров оценивается в 150 млрд рублей на конец 2021 года.

Евгений Царев, менеджер RTM Group, заявил, что количество успешных атак в 2021 году увеличилось по сравнению с предыдущим годом, в основном за счет действий мошенников, а не хакеров. Он ожидает, что в 2022 году количество успешных атак увеличится как минимум на 30-40%, что объясняется развитием схем социальной инженерии и использованием новых инструментов [Генеральная прокуратура РФ].

Олег Седов, директор по развитию направления «Киберграмотность» компании «Ростелеком-Solar», отметил, что низкий уровень киберграмотности населения делает его уязвимым для атак. Седов подчеркнул, что россияне стараются экономить, чем активно пользуются злоумышленники. Поэтому эффективность атак в 2022 году вряд ли снизится.

МВД сообщило о значительном сокращении числа некоторых преступлений, совершенных с использованием электронных средств в 2022 году. Статистика показывает снижение на 27,6% краж, на 29% мошенничества с использованием электронных методов оплаты и на 22,5% преступлений, связанных с компьютерной информацией.

Однако на 21% увеличилось число зарегистрированных преступлений, связанных с продажей наркотиков через Интернет. Кроме того, увеличилось число ложных сообщений о терроризме, причем 92% из них были совершены дистанционно. Положительным моментом является то, что раскрываемость преступлений, совершенных с использованием цифровых технологий, в 2022 году увеличилась на 4,4%.

В целом количество зарегистрированных преступлений в 2022 году снизилось на 1,9% по сравнению с предыдущим годом, а правоохранительными органами за этот период было раскрыто более 1 млн преступлений.

Как сообщают «Известия», положительная динамика в снижении преступлений, совершенных с использованием информационно-телекоммуникационных технологий, в том

числе пластиковых карт, мобильной связи и компьютерной техники, обусловлена повышением информированности населения о методах преступников, а также снижением криминальной активности весной 2022 года в связи со спецоперацией России на Украине. Тем не менее, эксперты предупреждают, что эта тенденция вряд ли сохранится.

Министерство внутренних дел (МВД) РФ опубликовало статистику по уровню преступности в стране в конце января 2023 года, включая показатели нарушений закона, связанных с использованием информационных технологий. Согласно опубликованным данным, киберпреступность осталась на стабильном уровне в целом. Каждое четвертое преступление совершается с использованием высоких технологий, как указано на сайте МВД в их сообщении.

Следует отметить, что официальная статистика может не отражать весь масштаб проблемы, поскольку многие финансовые преступления могут остаться незарегистрированными или необнаруженными. Таким образом, фактическое количество финансовых преступлений в России, скорее всего, выше заявленных цифр [Количество киберпреступлений в России].

Кто является потенциальными жертвами финансовых мошенников

Финансовое мошенничество может быть нацелено на широкий круг лиц и групп, и потенциально жертвой может стать любой. Однако есть некоторые группы, которые особенно уязвимы для финансового мошенничества. К ним относятся:

Пожилые люди. Пожилые люди часто становятся жертвами финансового мошенничества, поскольку они могут быть более доверчивыми и менее технически подкованными, чем молодые люди. Мошенники могут использовать различные тактики, чтобы воспользоваться уязвимостью пожилых людей, например, предлагая поддельные инвестиционные возможности или выдавая себя за члена семьи, нуждающегося в финансовой помощи.

Лица с низким доходом. Люди с низким доходом могут быть более уязвимы для финансового мошенничества из-за их финансового отчаяния. Мошенники могут предлагать поддельные кредиты или инвестиционные возможности, обещая быструю отдачу, но на самом деле пользуясь финансовым положением человека.

Владельцы малого бизнеса. Владельцы малого бизнеса могут стать жертвами финансового мошенничества, поскольку они чаще готовы идти на риск, чтобы развивать свой бизнес. Мошенники могут предлагать поддельные кредиты или инвестиционные возможности, выдавая себя за законных инвесторов или кредиторов.

Иммигранты. Иммигранты могут быть особенно уязвимы к финансовому мошенничеству, поскольку они могут быть не знакомы с местной финансовой системой и могут иметь ограниченный доступ к законным ресурсам. Мошенники могут предлагать поддельную иммиграционную помощь или инвестиционные возможности, пользуясь неосведомленностью и уязвимостью человека.

Состоятельные люди. Состоятельные люди также могут стать мишенью для финансового мошенничества, поскольку у них могут быть большие суммы денег и активов, на которые могут нацелиться мошенники. Мошенники могут выдавать себя за законных финансовых консультантов или предлагать поддельные инвестиционные возможности, пользуясь доверием и финансовыми ресурсами человека.

В целом, любой человек потенциально может стать жертвой финансового мошенничества, и важно быть осведомленным о распространенных видах финансового мошенничества и предпринять шаги, чтобы защитить себя от этих мошенников [Галанов].

КИБЕРМОШЕННИЧЕСТВО

Основные виды кибермошенничества

Существует много различных видов кибермошенничества, и наиболее распространенные из них — это:

Фишинговые аферы. Фишинговые аферы предусматривают деятельность мошенников,

отправляющих электронные письма или текстовые сообщения, которые кажутся исходящими из законного источника, такого как банк или сайт электронной коммерции, с целью обманом заставить людей предоставить личную информацию или учетные данные для входа.

Атаки с использованием вредоносных программ. Атаки с использованием вредоносных программ связаны с тем, что мошенники заражают компьютер или мобильное устройство пользователя вредоносным программным обеспечением, таким как вирус или шпионское ПО, которое может быть использовано для кражи личной информации, регистрации нажатий клавиш или получения контроля над устройством.

Атаки с использованием программ-вымогателей. Атаки с использованием программ-вымогателей включают в себя заражение мошенниками компьютера пользователя или мобильного устройства вредоносным ПО, которое шифрует файлы пользователя, делая их недоступными. Затем мошенник требует выкуп в обмен на ключ расшифровки [Министерство финансов РФ].

Мошенничество с компрометацией деловой электронной почты (BEC). В мошенничестве с BEC участвуют мошенники, выдающие себя за руководителя компании или поставщика и запрашивающие банковский перевод или другую финансовую транзакцию у сотрудника или поставщика.

Мошенничество с онлайн-аукционами. Мошенничество с онлайн-аукционами связано с мошенниками, выдающими себя за законных продавцов на сайтах онлайн-аукционов, таких как eBay или Craigslist, и обманом заставляющими людей платить за товары, которые они никогда не получат [Никитина].

Инвестиционные аферы. Инвестиционные аферы включают мошенников, использующих поддельные веб-сайты или аккаунты в социальных сетях для продвижения мошеннических инвестиционных возможностей, обещающих высокую доходность, но ничего не приносящих.

Любовные аферы. Любовные аферы включают мошенников, создающих поддельные профили на сайтах знакомств или платформах социальных сетей с целью установления отношений с человеком, а затем запрашивающих деньги или личную информацию.

Это лишь некоторые из многих видов кибермошенничества, с которыми могут столкнуться частные лица и предприятия. Важно быть в курсе этих мошеннических действий и предпринимать шаги для собственной защиты – например, избегать подозрительных электронных писем или веб-сайтов, использовать надежные пароли и поддерживать антивирусное программное обеспечение в актуальном состоянии.

Какие технологии используются мошенниками

Мошенники используют различные технологии для осуществления своих мошеннических действий. Некоторые из распространенных технологий и приемов, используемых мошенниками [Российская ассоциация электронных коммуникаций]:

Подмена. Мошенники часто используют методы подмены, чтобы скрыть свою истинную личность и выдать себя за кого-то другого. Это может быть связано с использованием поддельных адресов электронной почты или номеров телефонов, которые кажутся законными.

Вредоносное ПО. Вредоносное ПО, такое как вирусы или шпионские программы, может быть использовано для получения несанкционированного доступа к компьютеру или мобильному устройству жертвы, кражи личной информации или захвата контроля над устройством.

Социальная инженерия. Мошенники часто используют методы социальной инженерии, чтобы обманом заставить людей предоставить личную информацию или предпринять другие действия. Это может включать выдачу себя за доверенное лицо, такое как представитель банка или правительственный чиновник, с целью завоевать доверие жертвы.

Фишинг. Фишинговые мошенничества включают использование поддельных веб-сайтов или электронных писем, которые кажутся законными, с целью обмана отдельных лиц с целью предоставления личной информации, такой как учетные данные для входа в систему

или номера кредитных карт.

Голосовой фишинг (вишинг). Мошенничество с вишингом связано с использованием телефона для обмана людей с целью предоставления личной информации или совершения других действий. Вишинг может предусматривать выдачу себя за представителя банка или другого доверенного лица и запрос личной информации по телефону.

Смишинг. Мошенничество с использованием смишинга предполагает использование текстовых сообщений для обмана отдельных лиц с целью предоставления личной информации или совершения других действий. К этой категории относится выдача себя за законную компанию или государственное учреждение и запрос личной информации с помощью текстового сообщения.

Ботнеты. Ботнеты — это сети зараженных компьютеров или мобильных устройств, которые контролируются мошенником. Эти ботнеты могут использоваться для осуществления различных мошеннических действий, таких как отправка спам-писем или проведение распределенных атак типа DDoS.

Это лишь некоторые из множества технологий и приемов, используемых мошенниками. Важно быть осведомленным об этих методах и предпринимать шаги для защиты себя от этих мошенников: избегать подозрительных электронных писем или веб-сайтов, использовать надежные пароли и поддерживать антивирусное программное обеспечение в актуальном состоянии [Росфинмониторинг].

Кто является целевой аудиторией кибермошенников

Целевая аудитория киберпреступников может сильно различаться в зависимости от их мотивов и конкретного вида киберпреступлений, которые они совершают. Перечислим некоторые распространенные целевые аудитории киберпреступников:

Физические лица. Киберпреступники могут быть нацелены на отдельных пользователей Интернета с целью кражи личной информации, такой как учетные данные для входа, номера кредитных карт или номера социального страхования. Они также могут быть нацелены на отдельных лиц для атак программ-вымогателей или для получения доступа к их устройствам в других целях.

Малый бизнес. Малые предприятия часто становятся мишенью киберпреступников, поскольку у них могут быть менее сложные средства защиты от кибербезопасности, чем у крупных организаций. Киберпреступники могут нападать на малые предприятия с целью кражи конфиденциальных данных или получения доступа к их финансовым счетам.

Крупные корпорации. Крупные корпорации также являются распространенной мишенью киберпреступников, которые могут попытаться украсть конфиденциальные данные, нарушить бизнес-операции или заняться корпоративным шпионажем.

Органы государственной власти также часто становятся мишенями киберпреступников, которые могут попытаться украсть конфиденциальные данные, нарушить работу правительства или участвовать в актах кибервойны.

Критическая инфраструктура. Киберпреступники могут также нацеливаться на критическую инфраструктуру, такую как электросети, транспортные системы или системы водоснабжения, чтобы вызвать широкомасштабные сбои или даже физический вред.

Важно, чтобы все частные лица и организации были осведомлены о потенциальных рисках, создаваемых киберпреступниками, и предпринимали шаги для защиты себя от этих угроз. Это может включать внедрение надежных мер кибербезопасности, таких как брандмауэры и антивирусное программное обеспечение, а также постоянное информирование о последних угрозах и тенденциях в области кибербезопасности [Федеральная служба безопасности РФ].

МЕРЫ ПО БОРЬБЕ С ФИНАНСОВЫМ МОШЕННИЧЕСТВОМ

Работа правоохранительных органов по предотвращению и пресечению финансовых преступлений

Правоохранительные органы в России несут ответственность за предотвращение и

пресечение финансовых преступлений, включая мошенничество, отмывание денег и другие финансовые правонарушения. В мероприятиях по предотвращению преступлений участвуют Министерство внутренних дел (МВД), Федеральная служба безопасности (ФСБ) и Следственный комитет Российской Федерации (СК РФ), Банк России, Росфинмониторинг.

МВД является главным правоохранительным органом, ответственным за предотвращение и расследование финансовых преступлений. В его состав входит ряд специализированных подразделений, включая Управление экономической безопасности и противодействия коррупции и Департамент по расследованию финансовых преступлений. Эти подразделения отвечают за расследование финансовых преступлений, выслеживание мошенников и арест активов, полученных незаконным путем.

ФСБ также участвует в усилиях по предотвращению и пресечению финансовых преступлений, особенно тех, которые связаны с национальной безопасностью. В нем есть ряд специализированных подразделений, включая Департамент по защите конституционного строя и борьбе с терроризмом, которые работают над предотвращением финансовых преступлений, которые могут представлять угрозу национальной безопасности.

СК РФ отвечает за расследование и судебное преследование всех тяжких преступлений в России, включая финансовые преступления. В нем есть специализированное подразделение - Главное следственное управление, которое отвечает за расследование финансовых преступлений и предъявление обвинений отдельным лицам и организациям, причастным к финансовым преступлениям.

В дополнение к этим ведомствам Центральный банк России также выполняет работы по предотвращению и пресечению финансовых преступлений. В нем имеется ряд специализированных подразделений, в том числе Департамент финансового мониторинга, который отвечает за мониторинг финансовых операций и сообщение о подозрительной деятельности правоохранительным органам.

В целом, работа правоохранительных органов по предотвращению и пресечению финансовых преступлений в России является постоянной, поскольку мошенники и другие преступники продолжают находить новые способы осуществления своей незаконной деятельности. Важно, чтобы эти ведомства работали вместе для обмена информацией, координации усилий и были в курсе последних тенденций и технологий, используемых мошенниками, что позволит эффективно бороться с финансовыми преступлениями в России [Центральный банк РФ].

Развитие системы кибербезопасности в России

Развитие кибербезопасности в России было приоритетным в последние годы, поскольку страна становится все более уязвимой к киберугрозам. Власти России предприняли несколько шагов по укреплению системы кибербезопасности страны, включая следующее:

Правовая база. В 2016 году государственная власть России приняла новый закон о кибербезопасности, который установил правовую базу для кибербезопасности и создал ряд новых нормативных актов и стандартов информационной безопасности.

Национальная стратегия кибербезопасности. В 2019 году Государственный аппарат России принял новую Национальную стратегию кибербезопасности, в которой излагается комплексный план по укреплению возможностей страны в области кибербезопасности и защиты от киберугроз.

Центры кибербезопасности. Власти РФ создали ряд центров кибербезопасности по всей стране, которые отвечают за мониторинг киберугроз и реагирование на них. Эти центры тесно сотрудничают с правоохранительными органами и другими правительственными организациями для защиты критической инфраструктуры и других ключевых активов.

Международное сотрудничество. Власти России также подчеркнули важность международного сотрудничества в борьбе с киберпреступностью. Она работала над установлением партнерских отношений с другими странами и международными организациями для обмена информацией, координации усилий и разработки общих стандартов кибербезопасности.

Инвестиции. Российская Федерация осуществила значительные инвестиции в кибербезопасность, включая финансирование исследований и разработок новых технологий, а также создание новых центров кибербезопасности и учебных программ.

Несмотря на эти усилия, кибербезопасность остается серьезной проблемой для России, поскольку киберугрозы продолжают развиваться и становятся все более изощренными. Стране необходимо будет продолжать инвестировать в свои возможности в области кибербезопасности и тесно сотрудничать с другими странами и организациями для эффективного решения этой сохраняющейся проблемы.

Укрепление правовых механизмов для борьбы с финансовым мошенничеством

Укрепление правовых механизмов борьбы с финансовым мошенничеством является ключевым приоритетом для российского правительства. В последнее время в этой области произошло несколько событий, включая следующее:

Усиленные меры наказания. Законодатель ужесточил наказания за финансовые преступления, включая мошенничество и отмывание денег. Это включает в себя более жесткие тюремные сроки и более высокие штрафы для отдельных лиц и организаций, осужденных за финансовые преступления.

Новые правила. Органы государственной власти также ввели новые правила и стандарты для финансовых учреждений и других организаций, чтобы помочь предотвратить финансовое мошенничество. Это включает требования к большей прозрачности финансовых операций и увеличению числа сообщений о подозрительной деятельности.

Укрепление правоохранительных органов. Власти работают над укреплением правоохранительных органов, участвующих в борьбе с финансовым мошенничеством. Это включает в себя повышение уровня подготовки и выделение ресурсов следователям и другому персоналу правоохранительных органов, а также более тесное сотрудничество между различными ведомствами и организациями.

Международное сотрудничество. Государственный аппарат России также подчеркнул важность международного сотрудничества в борьбе с финансовым мошенничеством. Это включает в себя тесное сотрудничество с другими странами и международными организациями в целях обмена информацией и координации усилий.

Технологические решения. Власти также инвестируют в технологические решения для борьбы с финансовым мошенничеством. Это включает разработку нового программного обеспечения и других инструментов, помогающих обнаруживать и предотвращать мошеннические действия, а также использование передовой аналитики и искусственного интеллекта для выявления потенциального мошенничества.

В целом, органы государственной власти применяют многогранный подход к борьбе с финансовым мошенничеством, включая как юридические, так и технологические решения. Важно, чтобы эти усилия продолжались, поскольку финансовое мошенничество остается серьезной проблемой в России и во всем мире.

ЗАКЛЮЧЕНИЕ

Таким образом, следует подытожить все рассмотренные в работе аспекты проблемы финансовых преступлений и кибермошенничества в России. Следует отметить, что государство активно работает над усилением мер по борьбе с этими проблемами. Однако, необходимо продолжать работу над улучшением правовых механизмов, повышением кибербезопасности и расширением сотрудничества с другими странами в этой в этой сфере. Только комплексный подход и взаимодействие всех участников, начиная от государства и заканчивая банками и обычными гражданами, позволят добиться существенного прогресса в борьбе с финансовым мошенничеством и киберпреступностью в целом. Кроме того, важно проводить образовательную работу среди населения, чтобы повышать осведомленность людей о том, как не стать жертвой мошенников и как защитить свои финансовые интересы в сети интернет. Особое внимание следует уделить развитию механизмов для обнаружения и наказания мошенников, а также защите прав и интересов потерпевших от финансовых

преступлений. Все эти меры, при соблюдении правовых норм, будут способствовать улучшению обстановки в области финансового права в России.

СПИСОК ЛИТЕРАТУРЫ

Ассоциация банков России. URL: https://www.abr.ru/ (дата обращения: 17.02.2023).

Банк России. URL: http://www.cbr.ru/ (дата обращения: 17.02.2023).

Галанов В. А., Галанов А. В. Финансовая грамотность, финансовая вера и финансовое мошенничество // Вестник Российского экономического университета им. Г. В. Плеханова. 2020. Т. 17, № 3 (111). С. 157—165.

Генеральная прокуратура РФ. URL: http://genproc.gov.ru/ (дата обращения: 17.02.2023).

Жданова О. В., Лабовская Ю. В., Дедюхина И. Ф. Финансовое мошенничество в современном мире // Государственная служба и кадры. 2020. № 4. С. 95—97.

Количество киберпреступлений в России. URL: https://goo.su/ICEm5 (дата обращения: 17.02.2023).

Министерство финансов РФ. URL: http://www.minfin.ru/ (дата обращения: 17.02.2023).

Никитина И. А. Финансовое мошенничество в сети Интернет // Вестник Томского государственного университета. 2010. № 337. С. 122—124.

Российская ассоциация электронных коммуникаций. URL: https://www.raec.ru/ (дата обращения: 17.02.2023).

Росфинмониторинг. URL: https://www.fedsfm.ru/ (дата обращения: 17.02.2023).

Федеральная служба безопасности РФ. URL: https://www.fsb.ru/ (дата обращения: 17.02.2023).

Центральный банк РФ. URL: https://www.cbr.ru/ (дата обращения: 17.02.2023).

Original article

Artyom A. BOGDANOV	bachelor's degree, Northern Institute of the All-Russian State University of Justice (Petrozavodsk, Russian Federation) *9637421111@mail.ru*

PREVENTION OF FINANCIAL FRAUD IN MODERN RUSSIA

Scientific adviser:
Nikolay V. Levkin
Paper submi11ed on: 03/30/2023;
Accep1ed on: 03/31/2023;
Published on: 15/04/2023.

Abstract. The purpose of this paper is to provide a comprehensive overview of financial fraud, which includes financial crime and cyber fraud. The paper covers potential victims of financial fraud, types of cyberfraud, and technologies used by fraudsters.

Keywords: financial fraud, financial crime, cyberfraud, cybersecurity, fraudsters

For citation Bogdanov A. A. Prevention of Financial Fraud in Modern Russia. *StudArctic Forum*. 2023; 8(1): 83—90.