ВСЕРОССИЙСКИЙ КОНКУРС НА ЛУЧШУЮ НАУЧНУЮ РАБОТУ СТУДЕНТОВ И ШКОЛЬНИКОВ ПО ГУМАНИТАРНЫМ НАУКАМ

«ВЕЛЕНИЕ ВРЕМЕНИ»

Направление: уголовное право

Тема: «Финансовое мошенничество и способы борьбы с ним»

Соискатель: Тисленко Милена Алексеевна

Научный руководитель: Тисленко Алена Олеговна

Место выполнения работы: муниципальное общеобразовательное учреждение город Джанкой Республика Крым лицей «Многоуровневый образовательный комплекс №2 имени Героя Советского Союза Марии Карповны Байды»

2025

Аннотация

Цель данной работы – выяснить, как финансовое мошенничество влияет на общество, предложить меры борьбы с ним.

Задачи:

1. Провести анализ причин и условий, способствующих мошенническим действия в финансовой сфере.
2. Изучить виды финансового мошенничества.
3. Разобрать механизмы противодействия финансовому мошенничеству в Российской Федерации и оценить их эффективности.

Актуальность работы обуславливается тем, что финансовое мошенничество является одним из самых распространенных преступлений в современном мире. Мошенники действуют во всех сферах социально-экономической деятельности. Механизмы мошенничества бывают самыми разнообразными и со временем становятся все более сложными. Для того чтобы сохранить свое имущество и здоровье, необходимо знать о способах предупреждения опасных ситуаций в жизни, во избежание ситуаций, в которых можно лишиться своей собственности.

Степень изученности: проблема финансового мошенничества в России достаточно изучена, ей посвящены многие научные публикации, в том числе докторские и кандидатские диссертации, но действующие способы борьбы с этим явлением не имеют должной эффективности.

Наш вариант решения проблемы- создание трехступенчатой стратегии противодействия финансовому мошенничеству на базе ИИ, охватывающей разные сферы жизни.

Выводы:

1. Современные технологии играют двоякую роль: с одной стороны, они предоставляют новые возможности для мошенников, а с другой — открывают пути для повышения безопасности и защиты пользователей. Эффективные инструменты мониторинга и анализа данных могут помочь в выявлении мошеннических схем на ранних стадиях.
2. Программы повышения финансовой грамотности должны быть направлены на различные возрастные группы и социальные слои, чтобы обеспечить защиту наиболее уязвимых категорий граждан.
3. Борьба с финансовым мошенничеством требует комплексного подхода, включающего образование, технологические инновации, законодательные инициативы и межведомственное сотрудничество.

Практическое применение научных знаний состоит в глубоком анализе данных в области экономики, специалисты способны разработать профили риска и, впоследствии, стратегии проверки личности, использовании искусственного интеллекта для создания системы борьбы с мошенничеством, повышении финансовой грамотности населения.

Содержание

Введение…….....4
РАЗДЕЛ 1 Теоретико-правовые основы квалификации финансового мошенничества…….....…..…….5
1.1 Определение и виды финансового мошенничества…….....6
1.2 Причины распространения и отличия финансового мошенничества……6
1.3 Криминологическая характеристика личности финансового мошенника…….7
РАЗДЕЛ 2 Современные состояние и условия финансового мошенничества в РФ……...10
2.1 Анализ динамики, уровня и структуры финансового мошенничества в РФ (за последние 5-7 лет)……..10
2.2 Актуальные схемы и тактики финансового мошенничества……11
РАЗДЕЛ 3 Последствия финансового мошенничества…….14
3.1 Влияние на экономику государства…….…….14
3.2Социальные последствия для граждан…….....14
РАЗДЕЛ 4Способы борьбы с финансовым мошенничеством……..15
4.1Законодательные меры и технологические решения ……..…...15
4.2Особенности расследования мошенничества с использованием сети интернет…….16
РАЗДЕЛ 5 Разработка механизмов противодействия финансовому мошенничеству в РФ и оценка их эффективности…….……18
5.1 Анализ действующей системы противодействия финансовому мошенничеству в РФ……..……..18
5.2Эмпирическое исследование: выявление уязвимостей и оценка осведомленности учащихся лицея……....……...…….……..20
5.3Разработка и моделирование комплексной модели противодействия финансовому мошенничеству……..20
5.4 Оценка экономической и социальной эффективности предлагаемой модели.……...…21
Выводы……...23
Заключение……24
Список литературы……...……25
Приложения...……26

ВВЕДЕНИЕ

Финансовое мошенничество является одной из наиболее острых и актуальных проблем современного общества, оказывающим значительное влияние на экономику на глобальном, национальном и локальном уровнях. С развитием технологий и роста объема цифровых операций, мошеннические схемы становятся все более изощренными и трудноулавливаемыми. Финансовое мошенничество приводит к тому, что мировая экономика теряет 2,6 трлн долларов. Эти средства составляют более пяти процентов глобального ВВП. Эти цифры привел Генеральный секретарь ООН Антониу Гутерриш.[9] В дополнение к ощутимым финансовым потерям мошенничество влечет за собой пагубные последствия для репутации соответствующей организации, что, в свою очередь, негативно влияет на ее способность обеспечивать качественную реализацию программ, устанавливать партнерские отношения с другими организациями и получать взносы. Таким образом, наличие эффективных механизмов предупреждения и выявления мошенничества и борьбы с ним имеет ключевое значение для защиты интересов организаций от этих негативных последствий.

Опираясь на актуальные данные и исследования, работа направлена на формулирование рекомендаций и стратегий, способствующих профилактике финансового мошенничества и уменьшению его последствий. Исследование подчеркивает важность сотрудничества между государственными органами, финансовыми учреждениями и общественностью в усилиях по борьбе с этим явлением.

В работе будут рассмотрены современные подходы к законодательному регулированию, технологии, используемые для выявления мошенничества, необходимость повышения уровня финансовой грамотности населения.

Цель нашей работы:

Выяснить, как финансовое мошенничество влияет на общество, предложить меры борьбы с ним.

Задачи нашей работы:

1. Провести анализ причин и условий, способствующих мошенническим действиям в финансовой сфере.
2. Изучить виды финансового мошенничества.
3. Разработать механизмы противодействия финансовому мошенничеству в РФ и оценить их эффективности

Гипотеза – использование современных технологий, таких как искусственный интеллект и машинное обучение, значительно увеличивает эффективность обнаружения и предотвращения финансового мошенничества.

Объект исследования – финансовое мошенничество в современном государстве.

Предмет исследования – законодательство Российской Федерации, которое устанавливает ответственность за совершение мошенничества.

Актуальность работы обуславливается тем, что финансовое мошенничество является одним из самых распространенных преступлений в современном мире. Мошенники действуют во всех сферах социально-экономической деятельности. Механизмы мошенничества бывают самыми разнообразными и со временем становятся все более сложными. Для того чтобы сохранить свое имущество и здоровье, необходимо знать о способах предупреждения опасных ситуаций в жизни, во избежание ситуаций, в которых можно лишиться своей собственности.

В работе использованы системно-структурный и статистический методы исследования, анализ документов и анкетирование, аналитическое чтение.

РАЗДЕЛ 1

ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ КВАЛИФИКАЦИИ ФИНАНСОВОГО МОШЕННИЧЕСТВА

1.1 Определение и виды финансового мошенничества

Мошенничество — в уголовном праве РФ одно из преступлений против собственности, ненасильственная форма хищения. Представляет собой завладение чужим имуществом или приобретение права на имущество путем обмана либо злоупотребления доверием (ст. 159 УК РФ). Квалифицированным является мошенничество, совершенное повторно или по предварительному сговору группой лиц, а также в крупных размерах, организованной группой или особо опасным рецидивистом.

Финансовое мошенничество представляет собой незаконное действие, направленное на завладение деньгами, имуществом или иными ценностями. В наше время существует множество видов такого явления, которые часто основываются на психологических манипуляциях и создании ложных надежд.

На первом месте среди объектов преступных посягательств, составляя 62%, исходя из статистических данных, стоят денежные средства, на втором месте, составляя 19%, — автотранспорт, далее — антиквариат (11%). Носильные вещи, некрупная техника, разного рода аппаратура занимают оставшуюся небольшую долю.[3]

Одним из наиболее распространенных форм мошенничества являются финансовые пирамиды, которые привлекают вкладчиков обещанием высокой доходности. В такие схемы деньги вкладчиков поступают от новых участников до тех пор, пока система не развалится из-за нехватки свежих инвестиций. Ярким примером такой схемы является известная пирамида Сергея Мавроди —МММ, которая обещала своим участникам большую прибыль за счет вкладов новых клиентов. Считается, что на созданном сайте в 1994 году пропали деньги примерно 15 млн вкладчиков. Якобы столько же россиян, жителей стран СНГ и Европы вложило в «МММ 2011» не менее 350 млрд рублей (оценка организаторов пирамиды). Новый проект Мавроди работает больше года, каждый день приближаясь к краху, — по прогнозам математиков, пирамида развалится в течение ближайших трех-четырех месяцев.[11] Мавроди был осужден по статье 159 УК РФ за мошенничество в крупном размере.

Скимминг — установка на банкоматы нештатного оборудования (скиммеров), которое позволяет фиксировать данные банковской карты (информацию с магнитной полосы банковской карты и вводимый пин-код) для последующего хищения денежных средств со счета банковской карты.

Другим распространённым видом мошенничества в экономической сфере являются инвестиционные схемы на финансовых рынках. Здесь неосмотрительные инвесторы могут убеждать людей вкладывать деньги в несуществующие или убыточные проекты, обещая им высокую доходность, хотя многие из таких проектов являются фантазией. Кредитные мошенничества возникают, когда заемщик вводит кредитора в заблуждение, предоставляя ложные сведения о своей кредитной истории, доходах или собственности. Банки и другие учреждения также могут стать жертвами таких схем, когда заемщики оформляют кредиты на чужие имена.

Фишинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей-логинами и паролями. Мошенничества с банковскими картами включают несанкционированный доступ к счетам, кражу карт и использование украденной информации для совершения покупок.

Правовые мошенничества осуществляются через ложные требования на имущество или подделку правоустанавливающих документов. Этот вид мошенничества особенно распространён в крупных корпорациях и финансовых институтах. [10]

1.2 ПРИЧИНЫ РАСПРОСТРАНЕНИЯ И ОТЛИЧИЯ ФИНАНСОВОГО МОШЕННИЧЕСТВА

Финансовое мошенничество — это одна из самых распространенных и опасных форм преступлений в современном мире. Оно может нанести серьезный ущерб не только отдельным гражданам и организациям, но и всей экономике страны.

Предпосылки роста финансового мошенничества в современном мире:

– увеличение объема финансовых транзакций у каждого из нас;

– снижение возраста участников товарно-денежных и иных видов сделок;

– разнообразие видов денег и ценных бумаг;

– увеличение объема сделок вне личного контакта участников (Интернет-торговля);

– исчезновение границ для свободного перемещения денег, товаров, услуг в процессе глобализации (рост транснациональной финансовой преступности);

– резкое ускорение процессов технологизации нашей жизни;

– отставание технологий защиты функционирования финансовых систем всех уровней перед кибермошенниками;

– поведенческий и интеллектуальный разрыв между организаторами мошеннических схем и другими участниками финансовых отношений;

– сверхвысокие доходы участников финансовых афер при весьма умеренном наказании в большинстве стран мира;

– несоответствие поведенческих стереотипов участников финансово-денежных отношений новому уровню рисков. [12]

В отличие от обычной кражи, финансовое мошенничество характеризуется намеренным завладением чужими деньгами, но осуществляется более "секретным" способом. Все мошенничества в финансовом секторе имеют одну общую черту. Преступники получают деньги без принуждения, с согласия самих людей.

Коррупция часто включает в себя взаимодействие между должностными и частными лицами или организациями, где происходит обмен услуг или денег за определенные действия или бездействия. В финансовом мошенничестве используются различные обманные схемы и манипуляции, часто без участия государственных органов или должностных лиц.

Хотя финансовое мошенничество и коррупция имеют некоторые общие черты, такие как обман и получение выгоды за счет других, они различаются по своим механизмам, целям и последствиям. Финансовое мошенничество чаще всего направлено на индивидуальную выгоду без участия государственных структур, тогда как коррупция включает в себя взаимодействие с властными структурами и может иметь более широкие социальные последствия.

1.3 КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ЛИЧНОСТИ ФИНАНСОВОГО МОШЕННИКА

Исследования уголовных дел демонстрируют, что лица, совершающие экономические преступления, значительно отличаются по своим социально-демографическим характеристикам от тех, кто совершает другие виды преступлений, что имеет криминологическое значение.

Традиционно анализ начинают с гендерной принадлежности. Анализ уголовных дел показывает, что экономические мошенничества совершаются преимущественно мужчинами (63%). Несмотря на преобладание мужчин, доля женщин, совершающих эти преступления (36%), значительно выше, чем доля женщин, совершающих преступления в целом по России (16%).

Такое соотношение объясняется различиями в социальных ролях, социальными факторами, влияющими на преступное поведение женщин, и психологическими особенностями, связанными с их биологией. Сфера экономической деятельности, где совершаются мошенничества, требует специальных знаний, что влечет за собой совершение преступлений как мужчинами, так и женщинами. Некоторые мошеннические действия совершаются с помощью лиц определенных должностей и профессий, в которых часто работают женщины (например, работники банков, государственных учреждений). Кроме того, женщины легче вовлекаются в преступную деятельность.

Исследования показывают, что женщины редко выступают в качестве организаторов мошеннических действий (5%), чаще в роли исполнителей или пособников. Следует отметить рост участия женщин в экономических мошенничествах. В структуре корыстной женской преступности доминируют преступления против собственности. Например, в 2000 году этот показатель составлял чуть более 55%, а сейчас приближается к 95%, то есть увеличился на 40%. Доля мужчин, совершивших преступления против собственности, в структуре корыстной мужской преступности в среднем составляет 95%. Однако динамика доли мужчин, совершивших преступления против собственности, по сравнению с 2000 годом практически минимальна и составляет примерно 2–5%. Таким образом, разница в показателях существенна. В настоящее время показатели доли преступлений против собственности в структуре корыстных преступлений примерно одинаковы как у мужчин, так и у женщин.

При анализе половой принадлежности экономического мошенника необходимо учитывать, что пол преступника не является прямой детерминантой. Половые признаки определяют поведение, и в зависимости от обстоятельств они приобретают криминальное значение.

Возрастные особенности личности преступника, совершающего экономические преступления, позволяют определить характерные черты противоправного поведения различных возрастных категорий. Общепринято мнение, что молодые люди более склонны к совершению преступлений под влиянием внезапных эмоциональных всплесков, агрессии и тому подобного. Также, значительная часть молодых правонарушителей вовлечена в общеуголовные преступления корыстной направленности, такие как кражи, грабежи и

разбойные нападения. Анализ возрастных особенностей важен для разработки эффективных стратегий профилактики и выявления экономических преступлений.

В России преобладающее большинство экономических преступлений совершается лицами зрелого возраста, обладающими опытом и социальным статусом. Согласно исследованиям, средний возраст экономического преступника значительно выше, чем у лиц, совершающих общеуголовные преступления, и составляет 30 лет и старше, а средний возраст в целом — 42 года.

Первичные данные свидетельствуют о следующем распределении возрастных групп преступников на момент совершения преступления: наибольшая доля приходится на лиц от 30 лет и старше (55,9 %), за которыми следуют лица в возрасте от 18 до 24 лет (22,8 %). Меньшие доли составляют лица от 25 до 29 лет (19,5 %) и от 16 до 17 лет (1,8 %).

Следует отметить, что возрастные характеристики различаются в зависимости от вида экономического мошенничества. Более молодые лица чаще совершают мошенничества, связанные с завладением товаром с последующей оплатой, получением потребительского кредита или фальсификацией страховых случаев. В таких преступлениях наиболее часто встречается возрастная группа от 26 до 35 лет.

Исследование показывает, что экономические преступления чаще всего совершаются лицами со средним образованием. За ними следуют преступники с высшим образованием, а затем лица со средним профессиональным образованием. Доля злоумышленников с начальным образованием или без него незначительна, что, вероятно, связано с недостатком знаний для совершения экономических махинаций.

Анализ отдельных видов экономических преступлений выявляет, что совершение наиболее сложных из них требует соответствующего уровня образования. Следовательно, важно учитывать не только общий уровень образования, но и его направленность для понимания криминальной активности.

Семейное положение экономического мошенника имеет существенное значение для криминологического анализа его преступной деятельности. В современном обществе наблюдается тенденция к уменьшению количества регистрируемых браков и росту разводов.

Н.С. Лейкина подчеркивала прямую взаимосвязь между качествами преступной личности и условиями ее становления в семье. [7] В.Н. Кудрявцев и А.М. Яковлев детально описывают влияние семейного фактора на формирование преступника [5] и совершение им противоправных деяний. [8]

Стоит отметить, что определенная часть экономических мошенников, состоящих в браке во время совершения преступления, объясняется их особыми качествами. Зачастую эти лица идут на преступление из-за материальных проблем в семье, стремясь удовлетворить ее нужды. Им присущи такие черты, как усердие, высокая социальная ответственность и тому подобное, что характерно для семейных людей.

Можно утверждать, что в настоящее время семья утратила свою силу как сдерживающий фактор. Это, вероятно, связано с переоценкой моральных принципов в обществе, искажениями в системе потребностей и мотивации, деформацией правосознания и прочим.

Данные о трудовой деятельности преступника играют важную роль в криминологической характеристике экономического мошенника. Этот аспект может иметь различные криминологические последствия. С одной стороны, высокий уровень безработицы служит прямой причиной увеличения преступности, особенно корыстной. С другой стороны, должность и место работы в некоторых случаях напрямую связаны с совершением экономического мошенничества, особенно когда речь идет о преступлениях, совершенных с использованием служебного положения (ч. 3 ст. 159 УК РФ).

РАЗДЕЛ 2

СОВРЕМЕННЫЕ СОСТОЯНИЕ И УСЛОВИЯ ФИНАНСОВОГО МОШЕННИЧЕСТВА В РФ

2.1 АНАЛИЗ ДИНАМИКИ, УРОВНЯ И СТРУКТУРЫ ФИНАНСОВОГО МОШЕННИЧЕСТВА В РФ (ЗА ПОСЛЕДНИЕ 5-7 ЛЕТ)

Изучение современного состояния мошеннических действий в финансовой сфере Российской Федерации позволяет выделить основные тенденции, оценить серьезность опасности и определить ключевые направления для борьбы с ней. Данный анализ целесообразно проводить, рассматривая три взаимосвязанные составляющие: изменение во времени, степень распространенности и структуру (соотношение различных видов). За последнее десятилетие в России наблюдается ярко выраженная нелинейная динамика с двумя основными трендами:

Значительный подъем кибермошенничества. Начиная с 2018-2019 годов, и особенно во время пандемии, резко увеличилось число происшествий, связанных с применением методов социальной инженерии и несанкционированным доступом к счетам. По данным Центробанка, объем хищений с использованием социальной инженерии ощутимо возрос. Динамика характеризуется:

-Увеличением общего количества зарегистрированных случаев.
- Ростом доли успешных краж, что свидетельствует об усложнении способов мошенников.
- Переходом каналов атак с SMS и электронной почты на мессенджеры и голосовые звонки.

Сокращение числа традиционных банковских мошенничеств, но рост их сложности. Благодаря внедрению систем защиты от мошенничества и биометрической идентификации в банковской сфере, уменьшилось количество успешных краж с использованием поддельных документов или скимминга. Однако оставшиеся случаи часто являются хорошо спланированными атаками с вовлечением внутренних сотрудников организаций. Степень проблемы в России характеризуется следующими показателями: абсолютные цифры, доля в общей массе преступлений в кредитно-финансовом секторе, соотношение попыток и успешных краж.

Согласно оценкам Банка России и правоохранительных органов, ежегодный объем убытков граждан и организаций от финансовых махинаций оценивается десятками и сотнями миллиардов рублей. При этом официальная статистика МВД, отражающая только возбужденные уголовные дела, значительно занижает реальные масштабы из-за скрытого характера данного вида преступлений.

Финансовый обман, особенно в его кибер-варианте, стал преобладающим типом преступлений против собственности в финансовой области. Уровень успешности атак мошенников, несмотря на принимаемые меры, все еще довольно высок, что говорит об их хорошей приспособляемости.

Структура денежного обмана в России существенно изменилась на разных уровнях за последние годы, и сегодня она выглядит следующим образом:

Преобладание мошенничеств на микроуровне (более 90% по числу инцидентов):

Вишинг (звонки от лже — банка): занимает ведущую позицию. Мошенники, применяя методы социальной инженерии и используя утечки данных, убеждают жертв перевести деньги на "безопасные" счета или установить приложение для удаленного доступа.

Кибермошенничество с использованием фишинговых ссылок и вредоносного ПО.

Сим—своппинг (перехват телефонного номера) для получения доступа к банковским приложениям и SMS-подтверждениям.

Значительную долю мошенничеств на среднем уровне занимает кредитное мошенничество и сохраняет свою актуальность, особенно в сегменте необеспеченного потребительского кредитования. Далее идут махинации в сфере господдержки и льготного кредитования (например, в рамках программ помощи МСП во время пандемии) и инвестиционный обман, который. активно развивается в сегментах крипто активов и доверительного управления, обещая слишком высокую доходность.

Серьезной проблемой на макроуровне является скрытый характер коррупционных схем, их выявление и доказательство требуют значительных усилий со стороны правоохранительных и контрольных органов. Манипуляции рынком и инсайдерская торговля на отечественном фондовом рынке фиксируются Центробанком, но случаи привлечения к ответственности единичны.

Изучение тенденций, масштабов и форм финансового мошенничества в России позволяет сделать вывод: на сегодняшний день доминирующей угрозой являются быстро меняющиеся кибермошенничества на микроуровне, которые опираются на манипулирование людьми. При этом преступления среднего и крупного масштаба продолжают оставаться скрытыми. Чтобы эффективно противостоять этим явлениям, требуется многогранная стратегия, включающая как просвещение широкой общественности, так и укрепление взаимодействия между государственными органами, а также развитие передовых технологий для выявления мошенничества в финансовых учреждениях и для регулятора.

2.2 АКТУАЛЬНЫЕ СХЕМЫ И ТАКТИКИ ФИНАНСОВОГО МОШЕННИЧЕСТВА

Одна из новых схем в 2025 году — обман с «возвращением» Visa и Mastercard. [18] Киберпреступники рассылают СМС, маскируясь под банки, с целью вынудить получателей к немедленной верификации по ссылке, обещая возобновление международных транзакций. Эти ссылки перенаправляют на фальшивые сайты, имитирующие подлинные банковские порталы, где невнимательные пользователи вводят свои конфиденциальные данные, которые затем попадают в руки злоумышленников. Кроме того, через эти ссылки на устройство может быть внедрено вредоносное ПО, позволяющее получить контроль над девайсом. Мошенники часто маскируют номера отправителей под банковские, например, начинающиеся с +900, для создания иллюзии легитимности.

Злоумышленники разработали множество способов проникновения в учетные записи пользователей на портале Госуслуги. Взломанные аккаунты позволяют похищать личную информацию и оформлять микрокредиты на имя жертвы. Один из приемов — звонки якобы от оператора связи с просьбой продлить договор, для чего требуется назвать код из СМС, который, в действительности, используется для входа в Госуслуги.

Другая схема — повторная продажа оператором старых номеров телефонов. Мошенник, приобретая такой номер, легко восстанавливает доступ к учетной записи жертвы на Госуслугах, используя одноразовый код. Поддельные уведомления от Госуслуг, ведущие на фишинговые

сайты, звонки от лже—сотрудников с предложением усилить защиту аккаунта, а также запросы кодов доступа — также в ходу.

Мошенничество, связанное с "Пушкинской картой", становится все более распространенным. В этой схеме мошенники выходят на подростков в социальных сетях и, обещая помочь в переводе средств с карты в наличные, обманным путем получают доступ к их личной информации. Злоумышленники убеждают пользователей в возможности быстрого и простого получения наличных денег. Чтобы "обналичить" средства, жертва должна предоставить полные данные карты, а также коды подтверждения, полученные в SMS-сообщениях.

Существуют новые схемы, связанные и с налоговыми вычетами. Мошенники звонят гражданам, представляясь сотрудниками Федеральной налоговой службы (ФНС). [18] Жертв убеждают оформить налоговый вычет, открыв новую банковскую карту и заполнив заявление на фишинговом «сайте» ведомства. Получив платежные данные, злоумышленники обманным путем выманивают средства. Для завоевания доверия используются фишинговые сайты, искусно имитирующие официальные ресурсы, и предложения оформить карту для получения социальных выплат. Злоумышленники рассылают поддельные квитанции ЖКХ с QR-кодами, ведущими на фальшивые версии сайтов, где пользователь вводит свои учетные данные. Помимо перенаправления на фишинговый сайт, QR-код может вести на форму оплаты, в результате чего средства поступают напрямую мошеннику.

Получив контроль над данными банковской карты, мошенники немедленно снимают все доступные средства. После этого они прекращают любое общение, блокируют контактные данные жертвы и удаляют свои учетные записи в социальных сетях, чтобы замести следы.

Мошенники нацелены на ближайших родственников своих жертв. Представляясь сотрудниками правоохранительных органов или финансовых учреждений, преступники звонят подросткам и сообщают ложную информацию о том, что их родителям якобы грозит уголовное преследование за незаконные финансовые операции. Испуганный ребенок, стремясь спасти своих родителей, готов выполнить любые требования. Злоумышленники вынуждают детей проводить "видеообследование" квартиры, демонстрировать на камеру все имеющиеся денежные средства и ценности, а затем передавать их курьеру для "проверки" и "декларирования". Подобные действия, совершенные под давлением, приводят к утрате семейных накоплений.

Так, в начале 2025 г. в Москве 14-летнего подростка заставили поверить в историю о «спасении родителей» и передать курьеру 300 тыс. рублей и иностранную валюту. [17]

В июле были зафиксированы случаи мошенничества, связанные с платформой MAX (она была представлена российским гражданам в качестве национального мессенджера). [17] Злоумышленники звонили, представлялись сотрудниками MAX и убеждали срочно зарегистрироваться в новом сервисе. Ссылаясь на интеграцию MAX с госсервисами, пользователя просили продиктовать код подтверждения из СМС. На самом деле код приходит с портала Госуслуг. Если сообщить его мошенникам, то они получат доступ к личным данным гражданина, его документам и финансам. Затем поступает второй звонок, и мошенники сообщают собеседнику, что его аккаунт «Госуслуг» взломали. Пугают оформлением кредитов и переводом денег на финансирование экстремистов. Чтобы защитить средства, жертва должна срочно перевести их на «безопасный счёт» или отдать наличные курьеру

NFC-кражи: как обманывают бесконтактно. Злоумышленники все чаще используют бесконтактные технологии для похищения денег с банковских счетов. Схема обычно

начинается со звонка, в котором мошенник представляется сотрудником банка или правоохранительных органов и сообщает о взломе учетной записи на портале «Госуслуг», подозрительных операциях или обвинениях в финансировании запрещенных организаций. Под предлогом защиты сбережений жертве предлагают установить на телефон специальную программу.

Затем обманным путем вынуждают приложить карту к телефону и ввести PIN-код. Мошенники уверяют, что это безопасно, так как карта остается на руках. На самом деле, приложение считывает данные карты через NFC и передает их преступникам, находящимся у банкомата. Они используют устройство с аналогичным приложением, которое терминал воспринимает как карту жертвы. После ввода PIN-кода мошенник получает доступ к личному кабинету жертвы и выводит все деньги.

Второй вариант такого мошенничества: мошенники звонят с неизвестных номеров в мессенджерах и сообщают о несанкционированных транзакциях или взломе аккаунта Госуслуг. Цель — напугать жертву и убедить установить «спасительное» приложение, которое присылают через мессенджер. Этот файл содержит вредоносное ПО, активирующееся на устройстве. После этого злоумышленник предлагает обналичить все средства и внести их на «защищенный счет» через банкомат, используя телефон с включенным NFC.

Мошенник диктует цифры, представляя их как подтверждение перевода на безопасный счет. На самом деле, это PIN-код от карты дропа, таким образом, жертва переводит деньги на чужой счет.

РАЗДЕЛ 3

ПОСЛЕДСТВИЯ ФИНАНСОВОГО МОШЕННИЧЕСТВА

3.1 ВЛИЯНИЕ НА ЭКОНОМИКУ ГОСУДАРСТВА

Финансовое мошенничество — это не просто преступление, это язва, подтачивающая фундамент глобальной экономики и подрывающая социальное благополучие миллионов людей. Его масштабы поражают: от мелких краж с банковских карт до сложных, многомиллионных схем, задействующих офшорные компании и международные сети.

Проблема финансового мошенничества представляет серьезную угрозу глобальной экономической стабильности и социальному благополучию, что требует тщательного изучения как академическим сообществом, так и профессионалами в сфере финансового сектора.

Игнорировать её – значит обрекать себя на серьезные экономические потери и социальную нестабильность. Современный мир, отмеченный стремительным развитием цифровых технологий и автоматизации, создал благодатную почву для процветания финансового мошенничества. Автоматизированные системы, призванные упростить жизнь и ускорить финансовые операции, одновременно стали лёгкой мишенью для злоумышленников.

На сегодняшний день сферой преступной деятельности становится экономика, что связано с развитием автоматизации многих сфер экономической и рыночной деятельности. Именно такая деятельность превратилась в угрозу экономической безопасности. Заметим, что преступления в сфере экономики представляют особую опасность для общества и государства в целом. Н. И. Корда [4] говорит о том, что подрыв экономической безопасности приводит к ослаблению национальной экономики государства.

Государство страдает от финансового мошенничества, поскольку оно может привести к снижению налоговых поступлений и увеличению расходов на правоохранительные органы и судебные системы для расследования и преследования мошенников. Финансовое мошенничество, особенно в виде уклонения от уплаты налогов, приводит к значительным потерям для государственного бюджета. Это усугубляет финансовые ресурсы, доступные для социальных программ, инфраструктурных проектов и других важных инициатив.

Финансовое мошенничество может способствовать росту теневой экономики, где сделки проходят вне правового поля. Это может негативно сказаться на официальной экономике и привести к дальнейшим потерям налоговых поступлений.

3.2 СОЦИАЛЬНЫЕ ПОСЛЕДСТВИЯ ДЛЯ ГРАЖДАН

Жертвы финансового мошенничества часто теряют значительные суммы денег, что может привести к ухудшению их финансового положения. Это может стать причиной долгов, банкротства и даже потери имущества. Люди, ставшие жертвами мошенников, могут испытывать стресс, тревогу, депрессию и чувство стыда. Эти последствия могут оказывать длительное влияние на качество жизни и психическое здоровье пострадавших.

Финансовое мошенничество приводит к утрате доверия финансовым учреждениям, государственным организациям и даже близким людям. Это снижает уровень социальной сплоченности и сотрудничества в обществе.

Люди, потерявшие деньги, могут начать избегать взаимодействий с окружающими, чувствуя себя обманутыми или стыдящимися своей ситуации, что приводит к изоляции и ухудшению социальных связей. Чрезвычайные случаи мошенничества могут приводить к общественному возмущению и требованию более строгих мер со стороны государства.

РАЗДЕЛ 4

СПОСОБЫ БОРЬБЫ С ФИНАНСОВЫМ МОШЕННИЧЕСТВОМ

4.1 ЗАКОНОДАТЕЛЬНЫЕ МЕРЫ И ТЕХНОЛОГИЧЕСКИЕ РЕШЕНИЯ

Многие страны вводят более строгие наказания за финансовые преступления, такие как мошенничество, отмывание денег и злоупотребление служебным положением. Увеличение сроков лишения свободы и штрафов служит сдерживающим фактором для потенциальных преступников. Для борьбы с финансовым мошенничеством создаются специальные органы, такие как финансовая полиция или агентства по борьбе с экономическими преступлениями. Эти структуры сосредоточены на расследовании финансовых преступлений и взаимодействии с другими правоохранительными органами.

Современные технологии, такие как искусственный интеллект и анализ больших данных, активно используются для выявления подозрительных транзакций. Законодательство требует от финансовых учреждений внедрения систем мониторинга и отчетности для повышения прозрачности операций.

Финансовые учреждения обязаны сообщать о подозрительных операциях и проводить должную проверку своих клиентов. Это помогает предотвратить использование финансовой системы для незаконных целей.

Финансовое мошенничество часто имеет транснациональный характер, поэтому международное сотрудничество становится необходимым. Законы и соглашения, такие как «Конвенция о борьбе с коррупцией», способствуют обмену информацией и совместным расследованиям.

Государственные программы по повышению финансовой грамотности населения помогают гражданам распознавать мошеннические схемы и защищать свои финансы. Образовательные инициативы также направлены на обучение сотрудников финансовых учреждений методам выявления мошенничества.

Международный проект «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации». Целью проекта является формирование у российских граждан разумного финансового поведения, обоснованных решений и ответственного отношения к личным финансам, повышение эффективности в сфере защиты прав потребителей финансовых услуг. Основные компоненты проекта:

1) Разработка стратегии повышения финансовой грамотности, мониторинг и оценка уровня финансовой грамотности и защиты прав потребителей.
2) Создание потенциала в области повышения финансовой грамотности.
3) Разработка и реализация образовательных программ и информационных кампаний по повышению финансовой грамотности.
4) Совершенствование защиты прав потребителей финансовых услуг.[13]

Программа по повышению уровня финансовой грамотности жителей Калининградской области начала работать в 2011 году. Программа была инициирована министерством финансов Калининградской в рамках проекта Минфина России и Всемирного банка «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации».

31 декабря 2020 года международный проект Минфина России и Всемирного банка был завершен. И в России стартовал второй этап реализации Стратегии повышения финансовой

грамотности населения в Российской Федерации на 2017-2023 годы. В Стратегии определены основные приоритеты, цели и задачи повышения финансовой грамотности населения. Основная задача стратегического документа - консолидация усилий и ресурсов федеральных и региональные органов исполнительной власти, Банка России, финансовых институтов, профессионального сообщества и научно-педагогических кругов для повышения финансовой грамотности граждан России. Этапы реализации и роль регионов в части финансового просвещения определены в "Дорожной карте" по реализации второго этапа Стратегии повышения финансовой грамотности в Российской Федерации на 2017–2023 годы.[14]

Законодательные меры борьбы с финансовым мошенничеством должны быть комплексными и адаптивными к изменяющимся условиям. Эффективное законодательство в сочетании с активным сотрудничеством между государственными органами, частным сектором и гражданами может значительно снизить уровень финансовых преступлений и защитить экономику страны.

4.2 ОСОБЕННОСТИ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ.

Расследование уголовных дел, связанных с мошенничеством, которое было совершено через интернет или с использованием мобильной связи, представляет собой значительную сложность. Это обусловлено тем, что предварительное следствие и органы, занимающиеся оперативно-розыскной деятельностью, сталкиваются с серьезными проблемами при обнаружении лиц, участвующих в мошеннических схемах.

Кроме того, существует и другая значительная проблема: многие пострадавшие от таких преступлений не стремятся обратиться за помощью к правоохранительным органам. На это повлияют различные факторы, включая отсутствие интереса в выявлении мошенника, особенно если ущерб невелик, а также недоверие к работе правоохранительных структур.

Еще одной сложностью, с которой сталкиваются органы предварительного следствия, является отсутствие единой практики в области определения территориальной подследственности по сообщениям о мошенничествах, совершенных через интернет и сотовую связь. Расследование таких преступлений сопряжено с трудностями, поскольку для получения доказательств необходимы специфические знания в области информационных технологий и телекоммуникаций. Несмотря на эти трудности, у следователей существует стандартный набор необходимых действий.

В первую очередь следует провести допрос жертвы, в котором помимо основных фактов совершенного мошенничества важно выяснить детали общения с мошенником, а также точную сумму украденных средств. В случае «телефонного» мошенничества нужно получить от потерпевшего описание голоса злоумышленника, его темпа речи, а также индивидуальные особенности: акценты, возможные дефекты речи, пол и возрастные характеристики. Если преступление произошло посредством интернет-переписки, то желательно приложить к протоколу допроса скриншоты этой переписки для дальнейшего расследования.

Если у потерпевшего имеются чеки, квитанции о переводе денежных средств, то следователю необходимо произвести выемку в соответствии со ст. 183 УПК РФ.

Каждый год мошенники разрабатывают новые методы совершения преступлений, что приводит к росту схем. В случае, если сайт мошенника подключается к VPN, его фактический IP-адрес не будет известен пользователям, и его IP-адрес может использоваться для преступной

деятельности до доступа к веб-сайту. Данный факт говорит о том, что лица, расследующие такого вида преступления, должны постоянно расширять объемы своих познаний в сфере информационно-коммуникационных технологий, чтобы мыслить на несколько шагов вперед, продумывая все уловки злоумышленников

Инициативы органов предварительного расследования по борьбе с кибер-мошенничеством требуют дополнительного внимания и прямого сотрудничества между следственными и оперативными подразделениями, одновременно активизируя усилия по борьбе с мошенничеством в Интернете. Необходимо оптимизировать деятельность органов предварительного расследования при производстве по уголовным делам о мошенничестве, совершенном с использованием сети Интернет. Для точного определения последовательности и содержания алгоритмических действий следователя в различных следственных ситуациях необходимо четко отработать действия алгоритма и определить порядок и содержание действий алгоритма.

РАЗДЕЛ 5

РАЗРАБОТКА МЕХАНИЗМОВ ПРОТИВОДЕЙСТВИЯ ФИНАНСОВОМУ МОШЕННИЧЕСТВУ В РФ И ОЦЕНКА ИХ ЭФФЕКТИВНОСТИ

5.1 АНАЛИЗ ДЕЙСТВУЮЩЕЙ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ В РФ

Согласно данным Банка России, в июле — сентябре 2025 года в России заметно усилилась активность финансовых мошенников. Объём средств, похищенных без добровольного согласия клиентов, достиг 8,18 млрд рублей, что на 29% выше, чем во втором квартале. И МВД, и ФСБ регистрируют увеличение поступающих заявлений, что обусловлено как общим ростом преступной активности, так и повышением уровня юридической осведомленности граждан. При этом, процент раскрываемости этих преступлений остается сравнительно невысоким. Различные экспертные оценки указывают на то, что лишь малая часть (10-20%) дел доходит до успешного судебного преследования. Банки вернули клиентам лишь 5,1% похищенных денег — около 417 млн рублей, что почти на треть ниже, чем средний показатель прошлых кварталов.

Эффективность раскрытия мошеннических действий, затрагивающих структуры МВД, ФСБ и Следственного комитета, является важным направлением противодействия преступности в Российской Федерации. Современные схемы мошенничества становятся всё более сложными, что требует значительных ресурсов и скоординированных усилий от правоохранительных органов для их раскрытия. Далее будет рассмотрена текущая ситуация с раскрываемостью этих преступлений и факторы, оказывающие влияние на данный процесс.

Основная масса граждан, пострадавших от мошеннических действий, первоначально обращается в органы МВД России, которые являются передовой линией в борьбе с этим видом преступности. Именно сюда поступает наибольшее количество заявлений о фактах мошенничества. Основной акцент в работе ведомства делается на расследовании распространенных и типичных преступлений, таких как телефонное мошенничество, хищение средств с банковских карт и интернет-мошенничество. В ключевых ролях выступают управление «К», специализирующееся на борьбе с киберпреступлениями, включая фишинг, взлом и распространение вредоносного ПО.

Следственный комитет располагает более широкими полномочиями и ресурсами для проведения комплексных, многоэпизодных расследований, требующих тщательной проработки доказательной базы и координации действий в различных регионах. Основная задача СК РФ – выявление и привлечение к ответственности организаторов и бенефициаров преступных схем, до которых не всегда удается дойти на уровне МВД.

ФСБ России играет стратегическую роль в противодействии мошенничествам, представляющим угрозу экономической безопасности страны. В сферу ее внимания входят транснациональные преступные группировки, крупные схемы отмывания денежных средств, кибератаки на критическую инфраструктуру финансовой системы, а также противодействие финансированию экстремистской деятельности.

В идеале, данная система должна функционировать как единый механизм, в котором МВД занимается рядовыми случаями и предоставляет информацию для более глубоких расследований, СК РФ берет на себя сложные дела, а ФСБ наносит удары по стратегическим целям. Однако эффективность работы снижают проблемы взаимодействия между ведомствами, в том числе конкуренция за дела, разобщенность информационных систем и отсутствие

согласованности в оперативных действиях, что нередко позволяет организаторам масштабных мошеннических схем избегать ответственности.

Центральный банк Российской Федерации играет ведущую роль в процессе определения стратегии и координации деятельности по предотвращению финансовых махинаций на территории страны. Он не ограничивается контрольными функциями, а предполагает активное участие в создании безопасной финансовой среды. Оценка его работы через призму ключевых инициатив и нормативных документов позволяет выявить как стратегически значимые достижения, так и существующие системные трудности.

Изначально задуманная как проект, направленный на обеспечение финансовой независимости, карта «Мир» стала инструментом для повышения контроля над рынком платежей и внедрения унифицированных стандартов безопасности. С технической точки зрения, ЦБ получил возможность напрямую воздействовать на правила безопасности и механизмы мониторинга мошеннических операций для всей системы карт «Мир». Это дало возможность централизованно внедрять такие меры, как обязательная двухфакторная идентификация для онлайн-транзакций и единые алгоритмы анализа сомнительных операций. · Несмотря на высокий уровень защиты с применением технологий, карта «Мир» не смогла полностью решить проблему мошенничества, поскольку основные схемы переместились в область социальной инженерии, где вид используемой карты не играет решающей роли.

Учитывая риски быстрых и безотзывных переводов, Банк России с самого начала установил в СБП лимиты (первоначально 100 тыс. руб., впоследствии увеличенные), обязательное подтверждение транзакций через мобильное приложение банка-отправителя, а также собственную систему мониторинга мошеннических операций на стороне НСПК. Проблемы: СБП стала одним из основных каналов для злоумышленников из-за скорости и удобства использования. Регулирующий орган вынужден постоянно реагировать на новые угрозы, ужесточая лимиты, вводя обязательные задержки для первого перевода новому получателю, обязывая банки применять дополнительные проверки. Это является ярким примером противоречия между простотой использования сервиса и его безопасностью.

Указание Банка России № 5346-У является важным элементом защиты прав потребителей. Согласно этому регламенту банки обязаны возвращать клиентам средства в случае несанкционированных транзакций, если клиент не проявил "грубую небрежность" (не передавал реквизиты посторонним лицам, не сообщал ПИН-код и т.п.). Это создает мощный стимул для банков инвестировать в системы безопасности, поскольку убытки от мошенничества ложатся в первую очередь на них. Недостаток в том, что на практике возникает множество спорных ситуаций при интерпретации понятия "грубая небрежность". Клиенты, ставшие жертвами фишинговых атак или звонков от лже-сотрудников банка, часто добровольно предоставляют конфиденциальную информацию, что позволяет банкам отказывать в компенсации. Регулятору приходится постоянно давать разъяснения и уточнять толкование этих правил.

На мой взгляд, очень важным аспектом является деятельность Банка России по сбору информацию о всех случаях мошенничества от финансовых учреждений и выступление в качестве единого аналитического центра. Однако, даже при наличии централизации, скорость реагирования системы иногда отстает от скорости адаптации мошенников, которые постоянно меняют номера, реквизиты и методы. Кроме того, существует риск "ложных срабатываний" при автоматической блокировке операций добросовестных клиентов.

5.2 ЭМПИРИЧЕСКОЕ ИССЛЕДОВАНИЕ: ОЦЕНКА ОСВЕДОМЛЕННОСТИ НАСЕЛЕНИЯ

Цель анкетирования: оценить уровень финансовой грамотности школьников и администрации школы в контексте рисков мошенничества.

Гипотезы:

1. Уровень осведомленности граждан о схемах мошенничества обратно коррелирует с вероятностью стать жертвой.

2. Действующие системы фрод-мониторинга не успевают адаптироваться к появлению новых схем социальной инженерии.

В ходе работы нами было проведено анкетирование для выявления уязвимостей и оценки осведомленности населения. В опросе приняло участие 110 человек. Анкетирование проведено среди учеников старших классов и педагогического состава МОУ лицея «МОК №2 имени Героя Советского Союза Марии Карповны Байды». Опрос был анонимный.

1. Знакомы ли вам термины «фишинг», «вишинг»? А)Да Б)Нет. Положительно ответило 65 опрошенных и 45 — не знакомы с такими понятиями.

2. Узнаете ли вы типичные фразы мошенников («блокировка счета», «подозрительная операция»)? 93 респондента отметили «да» и 17 человек сомневаются: это мошенники или действительно техническая поддержка организаций. (Приложение А).

3. Как вы поступаете при звонке от якобы сотрудника банка? 72 анкетируемых ответили «сбрасываю вызов», 13 — отвечаю с целью развлечения», остальные 25 не получали таких звонков. (Приложение Б).

4. Проверяете ли вы адрес сайта перед вводом данных? — 91 голос «нет» и всего лишь 19 голоса за «проверяю».

5. Сталкивались ли вы мошенничеством? Сталкивались с попытками мошенничества 60 человек, респондент или его родственник стали жертвами — 23 человека и только 14 обращались в банк, 5 в полицию. Не сталкивались лишь 10 опрошенных. (Приложение В)

6.Кто чаще становится жертвами мошенничества на сегодняшний день?

А)подростки Б)зрелый возраст В)старшее поколение. По вопросу о возрасте потенциальных жертв, подавляющее большинство голосовало за старшее поколение — 65, за зрелый возраст — 36 и наименее подверженными считают подростков — 20 голосов.

Проведенный опрос выявил тревожную ситуацию и системные пробелы в финансовой грамотности респондентов, что свидетельствует об их высокой уязвимости перед мошенническими действиями. Несмотря на частичное знакомство с угрозами, на практике преобладают рискованные модели поведения. Гипотезы подтверждены.

5.3 РАЗРАБОТКА И МОДЕЛИРОВАНИЕ КОМПЛЕКСНОЙ МОДЕЛИ ПРОТИВОДЕЙСТВИЯ ФИНАНСОВОМУ МОШЕННИЧЕСТВУ

На основе выводов эмпирического анализа формируется многоуровневая стратегия борьбы с мошенничеством, объединяющая профилактические, оборонительные и репрессивные подходы. Модель охватывает три сферы воздействия: технологическую, юридическую и административную, плюс образовательный компонент.

Первый уровень — технологический — адресован банкам и фирмам в сфере финтеха. Здесь рекомендуется ввести анализ поведенческой биометрии, отслеживающий стиль ввода текста и перемещение мыши для обнаружения отклонений в поведении клиентов. Кроме того,

предполагается создание прогнозирующих моделей на базе ИИ, которые будут оперативно подстраиваться под свежие виды афер. Ключевым аспектом станет формирование отраслевого пула кибербезопасности для обмена сведениями о сомнительных транзакциях и IP-адресах аферистов, с учетом норм Федерального закона № 152 «О персональных данных».

Второй уровень — юридический и административный — фокусируется на действиях государства. Основной упор на нормативные нововведения, включая усиление наказаний за разработку и распространение вредоносного ПО, а также введение термина «цифровая идентичность». Административные шаги включают учреждение межведомственного центра по противодействию киберпреступлениям при МВД или ЦБ РФ с прямыми связями с финансовыми организациями. Дополнительно требуется оптимизировать процедуры для быстрого возмещения убытков жертвам по упрощенной схеме при явных индикаторах мошенничества.

Третий уровень — образовательный — нацелен на общество. Предусматривается запуск федеральной кампании по развитию финансовой осведомленности в рамках «Национального проекта «Финансовая безопасность». Планируется создание онлайн-симуляторов для тренировки в выявлении афер и обязательные разъяснения для пользователей при активации новых банковских сервисов.

В итоге, разработанная многоуровневая структура противодействия аферам интегрирует разнообразные инструменты для охраны банков и населения, усиливая общую защиту в финансовой отрасли.

5.4 ОЦЕНКА ЭКОНОМИЧЕСКОЙ И СОЦИАЛЬНОЙ ЭФФЕКТИВНОСТИ ПРЕДЛАГАЕМОЙ МОДЕЛИ

Введение многоуровневой системы борьбы с финансовым мошенничеством является важным шагом для улучшения экономической и социальной отдачи в области финансовых услуг.

С экономической стороны ключевым эффектом от применения прогнозирующих моделей ИИ и формирования единого киберцентра станет уменьшение прямых убытков. Согласно расчетам, это поможет остановить 70-80% мошеннических схем, что при ежегодных потерях населения в 20 — 25 млрд рублей и более даст возможность сэкономить примерно 15 млрд рублей в год. Автоматизация мониторинга мошенничества и введение анализа поведенческой биометрии сократят расходы банков на 25 — 30%, обеспечив дополнительную выгоду в 3 — 5 млрд рублей ежегодно за счет сокращения персонала и роста эффективности.

Затраты на создание и запуск ИИ-систем, межведомственный центр и образовательные инициативы оцениваются в 8 — 12 млрд рублей. При умеренной оценке годовой выгоды в 18 — 20 млрд рублей проект окупится за 1 — 1,5 года, а ROI превысит 100% в первые три года. Дополнительные эффекты, включая разгрузку правоохранителей и рост доверия к финансам, укрепят общую экономику.

Социальная модель повысит защиту граждан, уменьшив число жертв мошенничества на 50 — 60% за 2-3 года. Упрощение возврата средств по "беспроцессуальной" схеме и обучение цифровой гигиене для 70 — 80% населения создадут надежную финансовую среду. Уточнение понятия "цифровой личности" в праве устранить неясности, а ужесточение наказаний за киберпреступления усилит сдерживание.

В долгосрочной перспективе вырастет финансовая грамотность, снизится напряженность от убытков и сформируется культура кибербезопасности для всех возрастов.

Риски включают сбои в ИИ (15 — 20% шанс задержек), сопротивление в госструктурах и нужду в обновлении программ.

В итоге, многоуровневая система — эффективное решение с быстрой окупаемостью и широким положительным влиянием на общество и экономику. Ее внедрение оправдано и коммерчески, и на государственном уровне.

ВЫВОДЫ

В ходе исследования темы борьбы с финансовым мошенничеством было установлено, что это явление представляет собой серьезную угрозу для экономики и благосостояния граждан. Мошенничество в финансовой сфере принимает различные формы, включая инвестиционные схемы, фальшивые кредиты и онлайн-аферы, что делает его сложным для выявления и предотвращения.

Современные технологии играют двоякую роль: с одной стороны, они предоставляют новые возможности для мошенников, а с другой — открывают пути для повышения безопасности и защиты пользователей. Эффективные инструменты мониторинга и анализа данных могут помочь в выявлении мошеннических схем на ранних стадиях.

Для эффективной борьбы с финансовым мошенничеством необходима координация действий между государственными органами, финансовыми учреждениями и правоохранительными органами. Совместные усилия могут привести к более эффективному обмену информацией и лучшему реагированию на возникающие угрозы.

Ключевым элементом борьбы с финансовым мошенничеством является внедрение новых технологий в систему правоохранительных органов.

Не менее важна образовательная работа среди населения. Программы повышения финансовой грамотности должны быть направлены на различные возрастные группы и социальные слои, чтобы обеспечить защиту наиболее уязвимых категорий граждан.

В заключение, борьба с финансовым мошенничеством требует комплексного подхода, включающего образование, технологические инновации, законодательные инициативы и межведомственное сотрудничество. Только совместными усилиями можно создать безопасную финансовую среду, защищающую граждан от мошеннических схем и обеспечивающую устойчивое развитие экономики. В нашей исследовательской работе по борьбе с мошенничеством предлагаем прагматичный подход, избегая дорогостоящих и рискованных экспериментов с радикально новыми структурами. Вместо этого, он фокусируется на оптимизации существующих механизмов контроля и внедрении принципа пропорциональности реагирования на угрозы. Это означает, что масштабы противодействия должны соответствовать уровню риска.

ЗАКЛЮЧЕНИЕ

Подводя итог проделанной работе, посвященной исследованию проблемы финансового мошенничества и способам борьбы с ним, можно констатировать достижение поставленных задач и подтверждение выдвинутых теоретических предположений.

Эмпирическая часть исследования, включавшая опрос учащихся лицея, позволила объективно оценить осведомленность о распространенных мошеннических схемах и определить степень их подверженности риску. Результаты верификации гипотез оказались следующими: первая гипотеза, предполагавшая прямую зависимость между недостаточной информированностью и повышенной вероятностью стать жертвой, не получила статистического подтверждения. Это свидетельствует о том, что в современных условиях простого информирования о мошеннических схемах недостаточно, поскольку злоумышленники прибегают к сложным методам социальной инженерии, способным ввести в заблуждение даже осведомленных лиц. Вторая гипотеза полностью подтвердилась: существующая система оперативного мониторинга не успевает адекватно реагировать на быстрое появление и модификацию новых методов социальной инженерии, что создает критические уязвимости.

На основании полученных данных была сформирована комплексная модель противодействия финансовому мошенничеству, предусматривающая три взаимосвязанных этапа. Данный подход отличается системностью и охватывает все ключевые аспекты взаимодействия:

Первый уровень - технологический, ориентированный на финансовые учреждения и компании, предполагает внедрение передовых алгоритмов защиты и адаптивных систем контроля мошенничества на базе искусственного интеллекта.

Второй уровень – административно-правовой, фокусируется на мерах государственного регулирования, направленных на усиление контроля, ускорение блокировки подозрительных операций и усовершенствование законодательства.

Третий уровень - образовательный, сфокусированный на населении, смещает акцент с пассивного информирования на формирование критического мышления и навыков безопасного цифрового поведения.

Оценка экономической и социальной эффективности предложенной модели продемонстрировала, что ее внедрение не только снизит прямые финансовые потери граждан и бизнеса, но и значительно укрепит доверие к цифровой финансовой среде. Взаимодействие технологических инструментов, правовых ограничений и повышения уровня "цифровой гигиены" населения создает комплексный барьер, способный, в отличие от линейных решений, адаптироваться к постоянно меняющимся мошенническим схемам. Таким образом, реализация данной трехуровневой модели является насущно необходимой мерой для минимизации угроз финансовой безопасности как государства, так и его граждан.

СПИСОК ЛИТЕРАТУРЫ

1. Уголовный кодекс Российской Федерации
2. Уголовно-процессуальный кодекс Российской Федерации
3. Ковбенко Н. Д. Состояние и структура мошенничества в России // Российская юстиция, 2008. № 7.
4. Корда Н. И., Авраменко А. А. Мошенничество как угроза экономической безопасности страны // Молодой ученый. 2021. № 46 (388). С. 81–83.
5. Кудрявцев В.Н. Категория причинности в советской криминологии // Советское государство и право 1965. С. 8.
6. И.Г.Малкина-пых Психология поведения жертвы,2006. Стр. 6
7. Лейкина Н.С. Личность преступника и уголовная ответственность. Изд.: ЛОЛГУ им. А.А. Жданова, 1968. С. 14
8. Яковлев А.М. Некоторые теоретические вопросы изучения личности преступника / сб.: проблемы искоренения преступности. М.: Юридическая литература, 1965. С. 59.
9. https://news.un.org/ru/story/2018/12/1344641
10. https://nipkef.ru/about/blog/finansovoe-moshennichestvo-vidy-i-priznaki/
11. https://www.forbes.ru/investitsii/banki/80027-novaya-piramida-mavrodi-kogda-ona-ruhnet-i-komu-dostanutsya-dengi
12. https://adm.sseu.ru/content/otkrytaya-lekciya-finansovoe-moshennichestvo
13. https://minfin.gov.ru/ru/fingram/arhiv/international_project/about/description/
14. https://www.fingram39.ru/about/
15. http://static.government.ru/media/files/FJj6iZ8geL94xUACfr2s32ZQoUgqP7fd.pdf
16. file:///C:/Users/User/Downloads/sotsialno-demograficheskie-priznaki-lichnosti-ekonomicheskogo-moshennika.pdf
17. https://www.sberbank.ru/ru/person/kibrary/articles/top-10-aktualnykh-skhem-moshennichestva
18. https://www.gazprombank.ru/pro-finance/safety/novye-skhemy-moshennichestva/

ПРИЛОЖЕНИЯ

Приложение А

Рисунок 1

Рисунок 2

Приложение Б

Рисунок 3

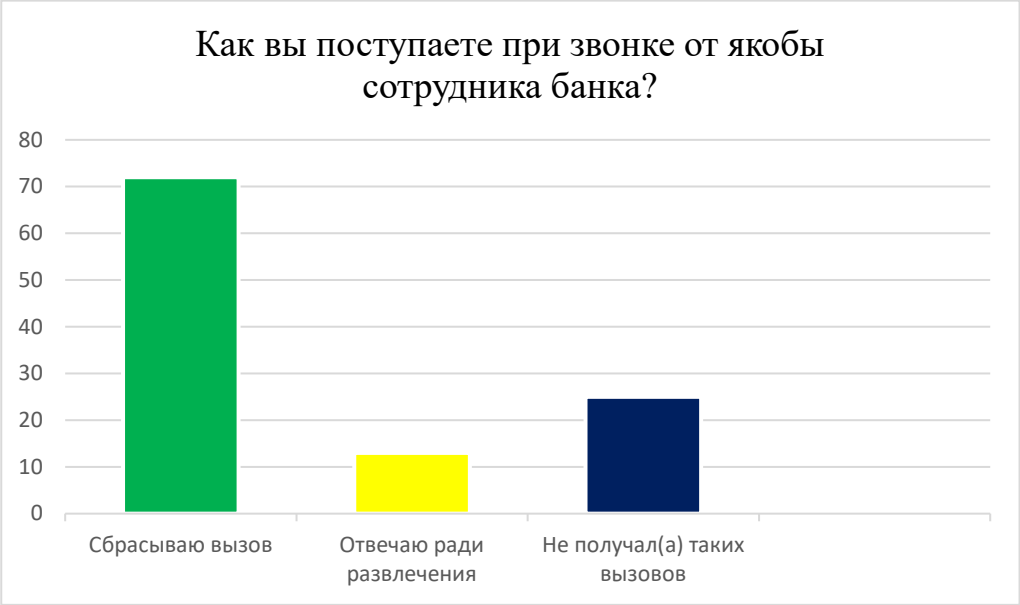

Рисунок 4

Приложение В

Рисунок 5

Рисунок 6