ВСЕРОССИЙСКИЙ КОНКУРС НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ И ТВОРЧЕСКИХ РАБОТ МОЛОДЁЖИ
«МЕНЯ ОЦЕНЯТ В XXI ВЕКЕ»

Направление: Экономика

Тема: «Финансовая безопасность и кибербезопасность»

Соискатели: Бардина Мария Андреевна, Субботин Максим Максимович

Научный руководитель: Ирина Николаевна Данилкина

Место выполнения работы: ЛДПК – филиал ГГТУ, Московская область, Ликино-Дулёво

2026 год

Аннотация

Работа посвящена исследованию финансовой безопасности личности в условиях роста кибермошенничества. Проанализированы современные схемы мошенничества, причины уязвимости граждан, правовые и технологические меры защиты. На основе анализа статистических данных и реальных кейсов выявлены ключевые тенденции и разработаны практические рекомендации по защите от кибермошенничества. Полученные результаты могут быть использованы в образовательных организациях, при проведении профилактических мероприятий и в семейном финансовом просвещении.

СОДЕРЖАНИЕ

Введение 4
Глава 1. Теоретические основы финансовой безопасности и кибермошенничества 6
1.1. Понятие финансовой безопасности: уровни и компоненты 6
1.2. Кибермошенничество: сущность, виды, эволюция 6
1.3. Правовое регулирование противодействия кибермошенничеству в РФ 7
Глава 2. Анализ современных угроз финансовой безопасности 9
2.1. Основные схемы кибермошенничества и их признаки 9
2.2. Психология жертвы: почему люди попадаются на уловки мошенников 9
2.3. Статистика и реальные кейсы 10
Глава 3. Аналитическое исследование методов противодействия кибермошенничеству и разработка рекомендаций 11
3.1. Анализ существующих методов защиты 11
3.2. Сравнительный анализ эффективности мер противодействия 11
3.3. Разработка памятки и рекомендаций по защите от кибермошенничества 11
Заключение 13
Список литературы 14
Приложение 15

ВВЕДЕНИЕ

Актуальность темы. Современный этап развития общества характеризуется стремительной цифровизацией финансовой сферы. Банковские операции, платежи, переводы, инвестиции всё чаще совершаются в электронном формате. По данным Банка России, ежегодно злоумышленники совершают миллионы операций без добровольного согласия клиентов, а объём похищенных средств исчисляется десятками миллиардов рублей[3]. Кибермошенничество превратилось в системную угрозу финансовой безопасности личности, бизнеса и государства.

Особую остроту проблеме придаёт постоянная эволюция схем обмана: мошенники осваивают искусственный интеллект, дипфейки, автоматизированные боты. При этом значительная часть населения не владеет элементарными правилами финансовой безопасности. Таким образом, возникает противоречие между необходимостью защиты граждан от кибермошенничества и недостаточным уровнем их финансовой грамотности и информированности о современных угрозах.

Проблема исследования: каковы эффективные способы защиты граждан от кибермошенничества и повышения их финансовой безопасности в условиях цифровизации?

Объект исследования: финансовая безопасность личности в условиях цифровой экономики.

Предмет исследования: кибермошенничество как угроза финансовой безопасности и методы противодействия ему.

Цель исследования: изучить современные угрозы финансовой безопасности, связанные с кибермошенничеством, и разработать практические рекомендации по защите граждан.

Задачи исследования:

1. Раскрыть понятие финансовой безопасности и её уровней.
2. Изучить сущность, виды и эволюцию кибермошенничества.
3. Проанализировать основные схемы обмана и причины уязвимости граждан.
4. Провести анализ существующих методов противодействия кибермошенничеству.
5. Разработать памятку и рекомендации по защите от кибермошенничества.

Гипотеза исследования: существующие методы противодействия кибермошенничеству недостаточно эффективны без активного участия самого гражданина, поэтому целенаправленное информирование и обучение способны существенно снизить риск стать жертвой обмана.

Научная новизна исследования заключается в следующем:

1. Систематизированы современные схемы кибермошенничества с учётом новейших технологий - дипфейков, ИИ-ботов, автоматизированного фишинга, которые ранее не рассматривались в комплексе в работах аналогичной направленности.

2. Проведён сравнительный анализ эффективности мер противодействия кибермошенничеству на трёх уровнях — личном, банковском и государственном, — что позволило выявить их взаимодополняющий характер.

3. Обосновано, что без активного участия самого гражданина технические и правовые меры защиты недостаточно эффективны.

4. Разработана и апробирована практическая памятка «10 правил финансовой безопасности», которая может быть использована в образовательных организациях и семейном просвещении.

Методы исследования: анализ научной литературы и нормативных актов, сравнение, обобщение, анализ статистических данных, кейс-метод, моделирование.

Практическая значимость: результаты работы могут быть использованы в школах, колледжах и вузах для проведения уроков и классных часов по финансовой грамотности, при разработке памяток для населения, в семейном просвещении.

Структура работы: работа состоит из введения, трёх глав, заключения, списка литературы и приложений.

Эмпирическая база исследования включает:

· аналитические доклады Банка России об операциях, совершённых без добровольного согласия клиентов;

· статистические сборники МВД России о состоянии преступности;

· данные Росфинмониторинга;

· реальные кейсы мошеннических операций, опубликованные в открытых источниках и средствах массовой информации;

· материалы проекта «Финансовая грамотность» Банка России;

· отчёты лаборатории Касперского и Positive Technologies о киберугрозах.

Анализ эмпирических данных позволил выявить ключевые тенденции в сфере кибермошенничества и обосновать практические рекомендации.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ФИНАНСОВОЙ БЕЗОПАСНОСТИ И КИБЕРМОШЕННИЧЕСТВА

1.1. Понятие финансовой безопасности: уровни и компоненты

Финансовая безопасность — это состояние защищённости финансовых интересов личности, общества и государства от внутренних и внешних угроз. Данное понятие включает три взаимосвязанных уровня.

В научной литературе существуют различные подходы к определению финансовой безопасности. Так, Ковалёв Д.В. рассматривает её как «способность личности противостоять финансовым угрозам и сохранять устойчивость в условиях нестабильной экономической среды» [5, с. 18]. Соколов А.В. акцентирует внимание на «совокупности условий, при которых гражданин может безопасно распоряжаться своими средствами и защищать их от противоправных посягательств» [6, с. 42].

Личная финансовая безопасность предполагает защиту личных сбережений, банковских счетов и персональных данных, а также способность человека противостоять финансовым манипуляциям. Это базовый уровень, от которого зависит благополучие конкретного гражданина. Личная финансовая безопасность включает несколько аспектов: сохранность денежных средств, защиту от несанкционированного доступа к счетам, конфиденциальность персональных данных, а также психологическую устойчивость к манипуляциям.

Корпоративная финансовая безопасность включает защиту активов компании, коммерческой тайны, платёжных систем, предотвращение внутреннего и внешнего мошенничества. Для бизнеса это критически важно, поскольку утечка данных или хищение средств могут привести к серьёзным потерям, вплоть до банкротства. Корпоративная безопасность обеспечивается комплексом мер: от технических средств защиты до обучения сотрудников.

Государственная финансовая безопасность обеспечивает устойчивость финансовой системы страны, борьбу с отмыванием денег, кибератаками на банковскую инфраструктуру и защиту национальных интересов. Этот уровень включает макроэкономическую стабильность, защиту национальной валюты, контроль за финансовыми потоками.

Основные компоненты финансовой безопасности:

· конфиденциальность — данные доступны только authorised лицам;

· целостность — информация и операции не искажены;

· доступность — сервисы работают бесперебойно;

· устойчивость — способность противостоять атакам.

Финансовая безопасность тесно связана с понятием финансовой грамотности. Чем выше уровень знаний гражданина в области финансов, тем выше его устойчивость к мошенническим схемам. Таким образом, личная финансовая безопасность — это не только техническая защита, но и результат образования и самодисциплины.

Вывод по параграфу: финансовая безопасность представляет собой многоуровневую систему, в которой личная безопасность гражданина является фундаментом для безопасности общества и государства.

1.2. Кибермошенничество: сущность, виды, эволюция

Кибермошенничество — это совокупность противоправных действий, совершаемых с использованием информационно-коммуникационных технологий с целью хищения денежных средств или персональных данных.

Характерные черты кибермошенничества:

· анонимность преступника;

· дистанционность — контакт без личной встречи;

· психологическое воздействие на жертву;

· высокая скорость операций;

· сложность раскрытия.

Эволюция кибермошенничества прошла четыре этапа:

Первый этап (1990-е — начало 2000-х). С появлением интернета возникли первые схемы обмана. Наиболее известны «нигерийские письма», в которых якобы наследник богатого человека просил помочь перевести миллионы, обещая долю. Несмотря на наивность, схема работала.

Второй этап (2000-е). Развитие банковских карт и интернет-банкинга привело к появлению фишинга, скимминга и кардинга. Мошенники массово рассылали письма от имени банков.

Третий этап (2010-е). Распространение смартфонов и мессенджеров вызвало расцвет телефонного мошенничества, вишинга и смишинга. Появились организованные преступные группы.

Четвёртый этап (2020-е — настоящее время). Использование искусственного интеллекта, дипфейков и автоматизации. Атаки становятся персонализированными и труднее распознаются.

Основные виды кибермошенничества:

Фишинг. Мошенники создают поддельные сайты, письма или сообщения, чтобы выманить логины, пароли, данные карт. Разновидности: классический фишинг (массовые рассылки), спир-фишинг (целевые атаки), вишинг (телефонные звонки), смишинг (SMS), квишинг (QR-коды).

Социальная инженерия. Это манипулирование человеком с целью получения конфиденциальной информации. Приёмы: претекстинг (легенда), приманка (предложение выгоды), кви про кво (обмен услугами), шантаж и запугивание.

Мошенничество с банковскими картами. Включает скимминг, шимминг, кардинг, подмену карты, онлайн-мошенничество.

Интернет-мошенничество. Фейковые магазины, криптовалютные пирамиды, взлом аккаунтов, фейковые розыгрыши.

Телефонное мошенничество. Звонки от «банка», «полиции», «родственника в беде».

Новые технологии. Дипфейки, ИИ-боты, автоматизированные атаки.

Отдельно стоит выделить мошенничество с использованием социальных сетей. Злоумышленники создают фейковые профили, вступают в доверие, а затем просят деньги или данные карт. Также распространено мошенничество через онлайн-игры — продажа «игровой валюты» или аккаунтов с предоплатой.

Криптовалютное мошенничество занимает особое место: создаются фейковые биржи, «инвестиционные платформы», обещающие сверхдоходность. Отсутствие регулирования и анонимность транзакций делают этот вид особенно опасным.

Вывод по параграфу: кибермошенничество постоянно эволюционирует, что требует постоянного обновления методов защиты.

1.3. Правовое регулирование противодействия кибермошенничеству в РФ

В России действуют следующие нормативные акты:

· УК РФ, ст. 159.3 — мошенничество с использованием электронных средств платежа [1];

· УК РФ, ст. 159.6 — мошенничество в сфере компьютерной информации [1];

· ФЗ «О национальной платёжной системе» [2];

· ФЗ «О персональных данных»;

· ФЗ «Об информации, информационных технологиях и защите информации».

Важную роль играет Банк России, который разрабатывает методические рекомендации для кредитных организаций, ведёт статистику мошеннических операций, координирует взаимодействие банков и правоохранительных органов. С 2024 года вступили в силу изменения, обязывающие банки возвращать средства клиентам в ряде случаев [2].

Однако, как отмечают эксперты, правовое регулирование не всегда успевает за развитием технологий. Мошенники осваивают новые способы обмана быстрее, чем принимаются законы [7, с. 50].

Ответственность за кибермошенничество может быть административной, уголовной (до 10 лет лишения свободы) и гражданско-правовой (возмещение ущерба). С 2024 года в ряде случаев банки обязаны возвращать средства клиентам, пострадавшим от мошенников [2].

Отдельно стоит отметить роль Банка России, который разрабатывает рекомендации для кредитных организаций, ведёт статистику мошеннических операций и координирует борьбу с киберпреступностью.

Вывод по параграфу: правовая база в России развивается, но требует постоянного обновления в связи с появлением новых схем.

Вывод по главе 1: теоретический анализ показал, что финансовая безопасность — многоуровневая система, а кибермошенничество — динамично развивающаяся угроза, требующая комплексного подхода.

ГЛАВА 2. АНАЛИЗ СОВРЕМЕННЫХ УГРОЗ ФИНАНСОВОЙ БЕЗОПАСНОСТИ

2.1. Основные схемы кибермошенничества и их признаки

Схема 1. «Звонок из банка». Жертве звонит «сотрудник банка» и сообщает о подозрительной операции. Под предлогом защиты средств просит назвать код из SMS или перевести деньги на «безопасный счёт». Результат — потеря всех средств. Признак: банк никогда не просит коды и не предлагает «безопасные счета».

Схема 2. «Родственник в беде». Мошенник звонит от имени родственника или «полицейского» и сообщает, что близкий человек попал в беду. Нужны деньги «для решения вопроса». Жертва в панике переводит средства. Признак: положить трубку и позвонить родственнику напрямую.

Схема 3. «Выгодная инвестиция». Предлагают «гарантированный доход» через криптовалюты, акции, форекс. Сначала дают вывести небольшую сумму, чтобы вызвать доверие, затем требуют всё больше вложений. В итоге сайт исчезает. Признак: обещание высокой доходности без риска.

Схема 4. «Фишинговый сайт». Жертва переходит по ссылке из SMS или письма на сайт, копирующий банк. Вводит логин, пароль, код. Данные попадают к мошенникам. Признак: проверить адрес сайта, наличие HTTPS, официальное приложение банка.

Схема 5. «Дипфейк». С помощью ИИ мошенники подделывают голос или видео родственника, руководителя, известного человека. Просят перевести деньги. Признак: задать вопрос, на который знает только реальный человек; перезвонить.

Схема 6. «Купля-продажа на маркетплейсах». Мошенник размещает объявление о продаже товара по заниженной цене. Просит предоплату на карту физлица. После перевода исчезает. Или наоборот: «покупатель» присылает ссылку на «оплату» через поддельный сайт доставки. Признак: предоплата на личную карту, слишком низкая цена, отсутствие отзывов.

Схема 7. «Взлом аккаунта в мессенджере». Мошенник взламывает аккаунт в Telegram или WhatsApp и от имени друга просит в долг. Или предлагает «проголосовать» по ссылке, которая крадёт данные. Признак: позвонить человеку по другому каналу связи; не переходить по ссылкам.

Схема 8. «Социальные выплаты и компенсации». Мошенники сообщают о «положенной выплате» от государства и просят данные карты для «перечисления». Признак: государство не запрашивает данные карт через SMS или мессенджеры.

Вывод по параграфу: существует множество схем, но все они опираются на психологическое воздействие и невнимательность жертвы.

2.2. Психология жертвы: почему люди попадаются на уловки мошенников

Эффект срочности. Мошенники создают искусственный цейтнот: «Счёт заблокируют через 5 минут!». В состоянии стресса мозг отключает критическое мышление, и человек действует импульсивно.

Эффект авторитета. Человек доверяет «сотруднику банка», «полицейскому», «представителю госоргана». Форма, голос, терминология внушают доверие, и жертва не задумывается о проверке.

Эффект выгоды. Обещание быстрого дохода отключает осторожность. Жертва думает: «Это мой шанс», и теряет бдительность.

Эффект стыда. После обмана человек часто не обращается в полицию: «Как я мог поверить?». Это играет на руку мошенникам и снижает статистику раскрываемости.

Эффект доверия к технологиям. Люди верят, что банковское приложение, официальный сайт, SMS от банка — это всегда безопасно. Но мошенники подделывают всё.

Эффект социального доказательства. Если «все так делают» или «друг уже получил выгоду», человек легче поддаётся убеждению.

Вывод по параграфу: защита должна быть не только технической, но и психологической. Нужно учиться распознавать манипуляции.

2.3. Статистика и реальные кейсы

Статистика показывает, что ежегодно Банк России фиксирует сотни тысяч жалоб на мошеннические операции [3]. Средний ущерб на одного пострадавшего составляет от 10 до 50 тысяч рублей, но есть случаи потери миллионов. Большинство атак — телефонные звонки (вишинг). Пик активности приходится на праздники, выходные и кризисные периоды.

Кейс 1. Пенсионерка из Москвы получила звонок «из банка». Ей сказали, что мошенники пытаются оформить кредит на её имя. Под предлогом «спасения» она перевела 2 миллиона рублей на «безопасный счёт». Деньги исчезли.

Кейс 2. Молодой программист из Санкт-Петербурга вложил 1,5 миллиона в «инвестиционную платформу» с обещанием 30% годовых. Первые выплаты получил, затем вложил ещё — сайт исчез.

Кейс 3. Студентка из Казани перешла по ссылке из SMS «от банка», ввела данные карты. С карты списали 80 тысяч рублей — все накопления.

Кейс 4. Предприниматель из Екатеринбурга получил письмо якобы от налоговой службы с требованием оплатить «задолженность» по ссылке. Перевёл 300 тысяч рублей. Сайт оказался фишинговым.

Кейс 5. Житель Новосибирска получил в мессенджере сообщение от «руководителя» с просьбой срочно перевести деньги «на нужды компании». Использовался дипфейк — поддельное видео с голосом руководителя. Сотрудник перевёл 500 тысяч рублей.

Кейс 6. Пенсионер из Волгограда поверил в «компенсацию от государства» за ранее купленные лекарства. Мошенники запросили данные карты для «перечисления». В результате со счёта исчезли 150 тысяч рублей.

Кейс 7. Студент из Москвы нашёл объявление о продаже игровой приставки по цене вдвое ниже рыночной. Продавец попросил предоплату. После перевода 40 тысяч рублей аккаунт был удалён.

Таблица 1. Распределение мошеннических операций по видам по данным Банка России

Вид мошенничества	Доля, %	Тенденция
Телефонное мошенничество (вишинг)	45	Рост
Фишинг (сайты, письма)	25	Стабильно
Мошенничество в соцсетях и мессенджера	15	Рост
Интернет-магазины и маркетплейсы	10	Стабильно
Прочие виды	5	-

Вывод по параграфу: жертвами становятся все — независимо от возраста, образования, дохода.

Вывод по главе 2: анализ угроз показал, что основная уязвимость — сам человек, а схемы обмана постоянно совершенствуются.

ГЛАВА 3. АНАЛИТИЧЕСКОЕ ИССЛЕДОВАНИЯ МЕТОДОВ ПРОТИВОДЕЙСТВИЯ КИБЕРМОШЕННИЧЕСТВУ И РАЗРАБОТКА РЕКОМЕНДАЦИЙ

3.1. Анализ существующих методов защиты

Защита от кибермошенничества осуществляется на трёх уровнях.

Личный уровень. Гражданин использует сложные пароли, двухфакторную аутентификацию, проверяет сайты и номера, не сообщает коды из SMS, регулярно проверяет выписки. К личным мерам также относятся: установка антивируса, отказ от перехода по подозрительным ссылкам, использование официальных приложений банков.

Банковский уровень. Кредитные организации внедряют антифрод-системы, которые анализируют операции в реальном времени, блокируют подозрительные транзакции, используют биометрию, отправляют уведомления. Современные антифрод-системы способны выявлять нетипичное поведение клиента и приостанавливать операции до подтверждения.

Государственный уровень. Создаются киберполиция и специальные подразделения, принимаются законы о защите прав потребителей финансовых услуг, реализуются программы финансовой грамотности, блокируются мошеннические сайты и номера. Банк России ведёт активную работу по информированию населения.

Вывод по параграфу: защита носит комплексный характер, но её эффективность зависит от активности самого гражданина.

3.2. Сравнительный анализ эффективности мер противодействия

Для наглядности представим сравнительный анализ в виде таблицы.

Таблица 2. Сравнительный анализ методов противодействия кибермошенничеству

Уровень защиты	Меры	Сильные стороны	Слабые стороны
Личный Пароли	2FA, проверка ссылок, антивирус	Простота, доступность, не требует затрат	Зависит от дисциплины и знаний человека
Банковский Антифрод	биометрия, блокировка операций	Автоматизация, скорость реакции, охват клиентов	Мошенники постоянно ищут обходные пути
Государственный Законы	киберполиция, просвещение, блокировка сайтов	Системность, охват, правовая защита	Требует времени, ресурсов, координации

Анализ показывает, что ни один уровень в отдельности не обеспечивает полной защиты. Только сочетание всех трёх уровней даёт результат.

Вывод по параграфу: наиболее эффективна комплексная защита, где гражданин, банк и государство действуют согласованно.

3.3. Разработка памятки и рекомендаций по защите от кибермошенничества

На основе проведённого анализа разработана памятка «10 правил финансовой безопасности»:

1. Никогда не сообщай коды из SMS.
2. Никогда не переводи деньги на «безопасные счета».
3. Всегда проверяй номер звонящего.
4. Всегда перезванивай в банк по номеру с обратной стороны карты.
5. Не переходи по ссылкам из SMS и мессенджеров.
6. Не устанавливай приложения по просьбе незнакомцев.
7. Используй двухфакторную аутентификацию.

8. Проверяй сайты перед вводом данных.

9. Не верь обещаниям быстрого дохода.

10. Расскажи о правилах близким, особенно пожилым.

Рекомендации по возрастным группам

Для школьников и студентов:

· проводить уроки финансовой грамотности;

· объяснять схемы мошенничества на конкретных примерах;

· обучать правилам безопасности в интернете;

· раздавать памятки.

Для взрослого населения:

· информировать через СМИ и соцсети;

· проводить корпоративные тренинги;

· напоминать о правилах при оформлении банковских продуктов.

Для пожилых людей:

· проводить индивидуальные беседы;

· устанавливать на телефоны определители номера и антивирусы;

· подключать SMS-уведомления;

· объяснять, что банк никогда не просит коды.

Для государства:

· расширять программы финансового просвещения;

· ужесточать ответственность за кибермошенничество;

· развивать международное сотрудничество;

· блокировать мошеннические сайты и номера;

· поддерживать проекты по финансовой грамотности.

Вывод по главе 3: анализ методов противодействия подтвердил гипотезу — без активного участия гражданина защита неэффективна. Разработанная памятка может быть использована для профилактики.

ЗАКЛЮЧЕНИЕ

В ходе исследования достигнута цель и решены все задачи.

Основные выводы:

1. Финансовая безопасность — многоуровневая система, фундаментом которой является личная безопасность гражданина.

2. Кибермошенничество постоянно эволюционирует, осваивая новые технологии.

3. Основная уязвимость — сам человек, его психология и недостаточная грамотность.

4. Правовая база в России развивается, но требует постоянного обновления.

5. Анализ методов противодействия показал, что наиболее эффективна комплексная защита.

6. Разработанная памятка и рекомендации могут быть использованы для профилактики.

Практическая значимость: результаты работы применимы в школах, колледжах, вузах, при проведении профилактических мероприятий.

Перспективы исследования: изучение влияния ИИ на кибермошенничество, разработка интерактивных обучающих программ, исследование эффективности государственных программ финансовой грамотности.

СПИСОК ЛИТЕРАТУРЫ

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ст. 159.3, 159.6) [Электронный ресурс]. — Режим доступа: http://www.consultant.ru (дата обращения: 30.09.2026).

2. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платёжной системе» [Электронный ресурс]. — Режим доступа: http://www.consultant.ru (дата обращения: 30.09.2026).

3. Банк России. Обзор операций, совершённых без добровольного согласия клиентов : аналитический доклад. — М. : Банк России, 2025. — Режим доступа: https://www.cbr.ru (дата обращения: 30.09.2026).

4. Ковалёв Д.В. Кибербезопасность личности : практическое руководство. — СПб. : Питер, 2025. — 256 с.

5. Проект «Финансовая грамотность» Банка России [Электронный ресурс]. — Режим доступа: https://fincult.info (дата обращения: 30.09.2026).

6. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс]. — Режим доступа: http://www.consultant.ru (дата обращения: 30.09.2026).

7. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» [Электронный ресурс]. — Режим доступа: http://www.consultant.ru (дата обращения: 30.09.2026).

8. Министерство внутренних дел Российской Федерации. Состояние преступности в России : статистический сборник. — М. : МВД России, 2025. — Режим доступа: https://мвд.рф (дата обращения: 30.09.2026).

9. Соколов А.В. Финансовая грамотность : учебное пособие. — М. : КноРус, 2025. — 280 с.

10. Петрова Е.Н. Социальная инженерия как угроза финансовой безопасности // Вопросы кибербезопасности. — 2025. — № 2. — С. 12–21.

ПРИЛОЖЕНИЕ

Приложение А.



Рис. 1 «Памятка правил финансовой безопасности»

Приложение Б.

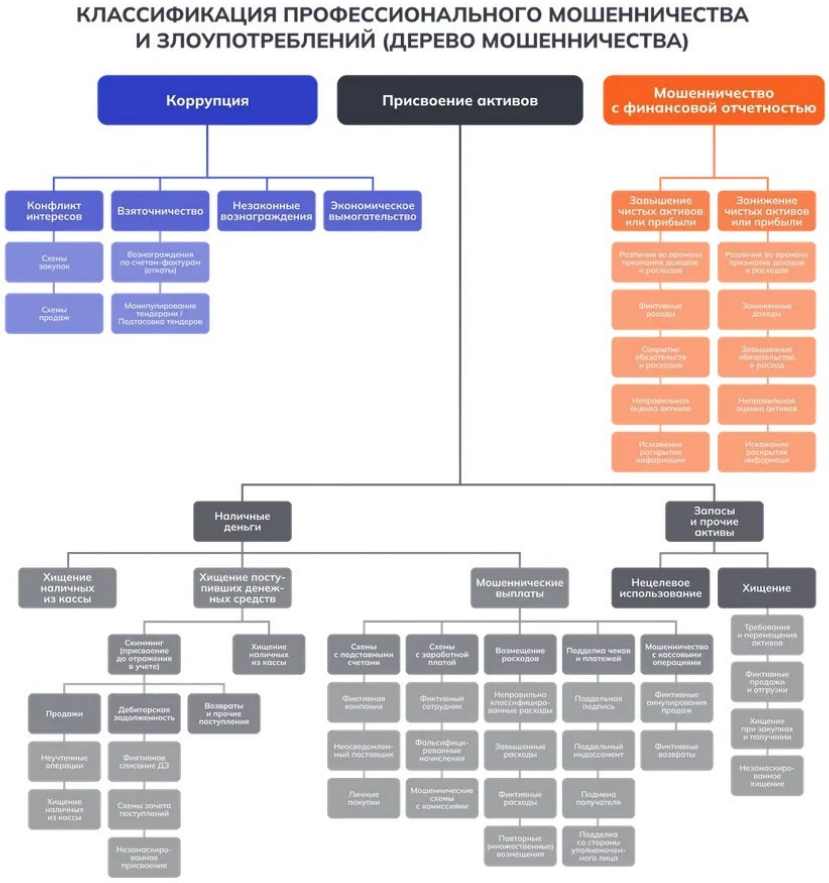


Рис. 2 «Сравнительный анализ методов противодействия»

Приложение В.



Рис. 3 «Схема уровни безопасности»