Мошенничество в цифровую эпоху: современные формы, механизмы противодействия и правовые аспекты.

Бахтуев Артем, Беляев Владислав, Прохоров Матвей, 2 курс. Гр.ЮРС-415,Сибирский университет потребительской кооперации (СибУПК), г. Новосибирск.

Аннотация

В работе представлен анализ мошенничества в условиях цифровизации общества. Рассмотрены эволюция и новые формы мошеннических схем (фишинг, кардинг, инвестиционные и романтические аферы в сети и т.д.). Объектом исследования выступают механизмы совершения преступлений, а субъектом – потерпевшие и правоприменительные органы. Цель работы – систематизация современных угроз и оценка эффективности мер противодействия. Результатом является разработка классификации мошеннических практик и предложения по совершенствованию законодательной базы и повышению цифровой грамотности населения.

Цель и задачи

Цель – разработка многоуровневой модели противодействия мошенничеству.

Задачи: 1) Классифицировать современные виды мошенничества; 2) Проанализировать правовые нормы; 3) Оценить эффективность профилактических мер.

Проблема

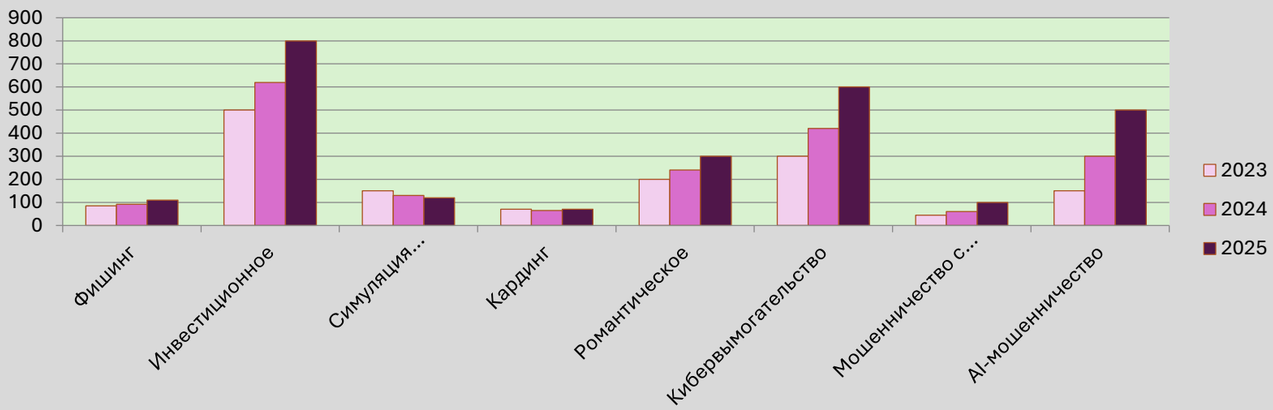
Глобализация и цифровизация создали новую среду для мошенничества, наносящую многомиллиардный ущерб экономикам и психологический вред гражданам.

Результаты и обсуждение

· Фишинг и социальная инженерия остаются основными векторами атак (до 70% инцидентов).
· Наблюдается рост сложных схем с использованием криптовалют и «социального взлома».
· Эффективность возврата средств по кибераферам не превышает 15-20%.
· Правовые нормы отстают от технологического развития методов мошенничества.

Обсуждение: Полученные данные согласуются с выводами Smith et al. (2022) о доминировании человеческого фактора как уязвимости. В отличие от классических схем, современное мошенничество часто транснационально, что требует усиления международного сотрудничества.

Динамика и прогноз мошенничества по ключевым категориям (с 2023-2025гг). Средний ущерб в тыс. рублей.



Определение мошенничеств

Инвестиционное мошенничество — схемы, в которых мошенники, представляясь финансовыми специалистами, завлекают жертв на поддельные платформы для вложения денег под обещание большой прибыли. Подобная деятельность, включая создание финансовых пирамид, регулируется статьёй 14.62 КоАП РФ.

Кардинг — несанкционированное использование украденных данных банковских карт для оплаты или снятия денег. Противодействие таким преступлениям связано с законом №115-ФЗ о противодействии отмыванию преступных доходов.

Романтическое мошенничество — построение ложных отношений в сети с целью получения денег или личной информации. Ответственность наступает по статье 159 УК РФ, а операции с полученными средствами могут подпадать под закон №115-ФЗ

Кибервымогательство — цифровой шантаж с угрозами утечки данных или кибератак. Преступление квалифицируется по статьям 159.6 («Мошенничество в сфере компьютерной информации») или 272 УК РФ.

Определение мошенничеств

Мошенничество с использованием аккаунта на «Госуслугах» — это неправомерный доступ к личным кабинетам пользователей с целью получения персональных данных и их использования в криминальных целях. Регулируется статьей 272 УК РФ— неправомерный доступ к компьютерной информации.

AI-мошенничество — это использование технологий искусственного интеллекта для создания поддельных видео и аудио, чтобы обмануть людей с целью вымогательства денег. В России рассматривается законодательство, направленное на противодействие мошенничеству с использованием ИИ.

Определение мошенничеств

Фишинг — вид интернет-мошенничества, целью которого является получение конфиденциальных данных (логинов, паролей, банковских реквизитов). За него предусмотрена уголовная ответственность по статьям 159 («Мошенничество») или 272 («Неправомерный доступ к компьютерной информации») УК РФ

Симуляция родственников — вымогательство денег под видом близкого человека, попавшего в беду. Данное мошенничество квалифицируется по статье 159 УК РФ.

Методы и материалы

1. Схема исследования: Дескриптивный и аналитический обзор, включая case-study.
2. Популяция/Образцы: Анализ открытых баз данных судебных решений (n=150), отчетов CERT, статистики Центробанка за 2020-2023 гг.
3. Локация: Исследование фокусируется на РФ с сравнительным анализом опыта ЕС и США.
4. Ограничения: Сложность получения закрытых данных правоохранительных органов; латентность преступлений.
5. Методика: Контент-анализ, сравнительно-правовой метод, статистический анализ.
6. Материалы: Научные публикации, законодательные акты (УК РФ), отчеты о мошенничестве.
7. Переменные: Вид мошенничества, сумма ущерба, категория жертвы, способ совершения, результат расследования.

Заключение

1.Обобщение: Мошенничество эволюционирует в сторону технологической сложности и психологической изощренности, эксплуатируя цифровую неграмотность и доверчивость.
2. Практическое применение: Необходимо:
· Внедрение обязательных модулей по цифровой гигиене в образовательные программы.
· Ужесточение регуляции анонимных финансовых операций.
· Создание единого оперативного центра по отслеживанию мошеннических схем.
3. Направление будущих исследований: Изучение возможностей AI и машинного обучения для предиктивного анализа и блокировки мошеннических операций в реальном времени, а также глубокий виктимологический анализ.