

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Пензенский государственный университет»

Юридический институт

Кафедра «Уголовное право»
(наименование)

Направление подготовки 40.03.01
(код)

Юриспруденция
(наименование)

Профиль «Правозащитная деятельность»
(наименование)

БАКАЛАВРСКАЯ РАБОТА

по теме: «Влияние новых технологий на развитие и распространение
мошеннических схем»

Студентка 21ЮЮ05
номер группы

подпись, дата

Очкина Елизавета Андреевна
фамилия, имя, отчество

Научный руководитель К.Ю.Н., доцент
должность

кафедра «УП» ФГБОУ ВО ПГУ
наименование организации

подпись, дата

Красковский Я. Э.
фамилия, инициалы

Консультанты:

по _____
наименование раздела, звание, должность

подпись, дата

фамилия, инициалы

по _____
наименование раздела, звание, должность

подпись, дата

фамилия, инициалы

по _____
наименование раздела, звание, должность

подпись, дата

фамилия, инициалы

Нормоконтролер: К.Ю.Н., доцент
должность

подпись, дата

Живодрова Н. А.
фамилия, инициалы

Работа допущена к защите в (протокол заседания кафедры от _____ 2025 № _)

Заведующий кафедрой «Уголовное право»
название

подпись, дата

Романовский Г. Б.
фамилия, инициалы

Работа защищена с оценкой _____ (Протокол от _____ 2025 г. № _____)

Секретарь ГЭК

подпись, дата

Антипкина Е. Г.
фамилия, инициалы

Пенза, 2025 г.

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Юридический институт

Направление 40.03.01 «Юриспруденция»

Профиль «Правозащитная деятельность»

УТВЕРЖДАЮ

Зав. кафедрой «Уголовное право»

_____/Г. Б. Романовский /
(подпись) (и.о. фамилия)

2025 г.

ЗАДАНИЕ

на выпускную квалификационную работу студентки гр.№21ЮЮ5
Очкиной Елизаветы Андреевны

1.Тема работы: Влияние новых технологий на развитие и распространение
мошеннических схем

2.Научный руководитель: к.ю.н., доцент каф. УП Красковский Я. Э.

3. Дата выдачи задания: 03.02.2025 г.

4. Срок сдачи слушателем законченной работы: 19.05.2025 г.

5. Перечень подлежащих разработке вопросов:

5.1 Современные технологии и их роль в мошенничестве

5.2 Типы мошеннических схем в цифровую эпоху

5.3 Социальные последствия цифрового мошенничества

5.4 Анализ реальных случаев мошенничества в Пензенской области

5.5 Расследование кибермошенничества

5.6 Методы противодействия новым технологиям в мошенничестве

5.7 Роль государства в борьбе с мошенничеством

5.8 Образование и осведомленность населения

5.9 Рекомендации по повышению мер безопасности

6. Консультанты по работе, с указанием относящихся к ним разделов работы:

Раздел	Консультант	Подпись, дата	
		Задание выдал	Выполненное задание принял
Введение		07.02.2025г. Красковский Я.Э.	17.02.2025г. Красковский Я.Э.
Современные технологии и мошенничество		17.02.2025г. Красковский Я.Э.	01.03.2025г. Красковский Я.Э.
Анализ и последствия мошенничества		01.03.2025г. Красковский Я.Э.	15.03.2025г. Красковский Я.Э.
Образование и безопасность		15.03.2025г. Красковский Я.Э.	31.03.2025г. Красковский Я.Э.
Заключение		31.03.2025г. Красковский Я.Э.	14.04.2025г. Красковский Я.Э.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	5
1 Современные технологии и мошенничество.....	7
1.1 Современные технологии и их роль в мошенничестве.....	7
1.2 Типы мошеннических схем в цифровую эпоху.....	10
1.3 Социальные последствия цифрового мошенничества.....	18
2 Анализ и противодействие мошенничеству.....	21
2.1 Анализ реальных случаев мошенничества в Пензенской области.....	21
2.2 Расследование кибермошенничества.....	23
2.3 Методы противодействия новым технологиям в мошенничестве.....	28
2.4 Роль государства в борьбе с мошенничеством.....	32
3 Образование и безопасность.....	36
3.1 Образование и осведомленность населения.....	36
3.1 Рекомендации по повышению мер безопасности.....	38
ЗАКЛЮЧЕНИЕ.....	41
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	44
ПРИЛОЖЕНИЕ А.....	49

ВВЕДЕНИЕ

Актуальность темы исследования заключается том, что современное общество находится в условиях стремительного технологического прогресса, развитие цифровых технологий, искусственного интеллекта, мобильных платформ и социальных сетей, которые открывают новые возможности для киберпреступности и мошенничества.

Мошеннические схемы эволюционируют вместе с развитием технологий, становясь более масштабными, автоматизированными и труднодоказуемыми. Традиционные схемы мошенничества устарели и уступили место современным кибермошенникам, использующим фишинг, социальную инженерию, deepfake- технологии и криптовалютные схемы. Все эти методы создают серьезную угрозу безопасности граждан, организаций и государству в целом.

Проблема усугубляется существенным разрывом между скоростью технологических изменений и адаптационными возможностями общества. Большинство граждан, особенно старших возрастных групп, демонстрируют критически низкий уровень цифровой грамотности, не позволяющий адекватно оценивать киберриски. При этом традиционные образовательные программы не успевают реагировать на появление новых угроз, таких как генеративный ИИ-фишинг или синтетическая идентификационная кража.

Исследование современных технологий как катализатора эволюции мошеннических схем представляет собой междисциплинарную проблему, находящуюся на стыке криминологии, киберпсихологии, цифрового права и технологического менеджмента. Его актуальность будет только возрастать по мере дальнейшей цифровизации общества и появления принципиально новых технологических платформ.

Объектом исследования являются современные мошеннические схемы в цифровом обществе.

Предметом исследования является влияние новых технологий на их развитие, распространение и методы противодействия.

Цель исследования состоит в комплексном анализе влияния новых технологий на развитие и распространение мошеннических схем, а также выработка рекомендаций по противодействию им.

Для достижения поставленной цели необходимо решить следующие задачи:

1. дать общую характеристику современных технологий и их роли в мошенничестве;
2. рассмотреть типы мошеннических схем в цифровую эпоху;
3. проанализировать реальные случаи мошенничества;
4. рассмотреть социальные последствия цифрового мошенничества;
5. выявить методику расследования кибермошенничества;
6. проанализировать методы противодействия новым технологиям в мошенничестве;
7. рассмотреть образование и осведомленность населения;
8. разработать рекомендации по повышению мер безопасности

Методологической основой работы является сочетание теоретических методов (анализ научной литературы, нормативно-правовых актов, статистики), эмпирических методов (изучение судебной практики), системный и сравнительный анализ.

Теоретической основой исследования явились труды ученых и специалистов в области уголовного права: Антонян Е. А., Аминов И. И., Баймедетов С. Д., Пак Л.Ю., Баишев Д. А., Данилова Е. П., Портняга Е. М. и многие другие.

Нормативно-правовой основой послужили Конституция РФ, УК РФ, международные конвенции и другие федеральные законы.

Структура работы обусловлена целью и задачами исследования и включает в себя настоящее введение, три раздела, объединяющие девять подразделов, заключение, список используемых источников и приложение.

1 Современные технологии и мошенничество

1.1 Современные технологии и их роль в мошенничестве

История появления кибермошенничества началась практически одновременно с развитием компьютерных технологий и интернета. В 1970-1980-х годах, когда компьютеры стали более доступными, а сети начали объединять пользователей, мошенники быстро адаптировали традиционные схемы обмана под цифровую среду ¹.

Одним из первых известных случаев кибермошенничества считается так называемая «схема с телефонными звонками», когда преступники использовали уязвимости в телефонных сетях для бесплатных междугородних звонков или доступа к платным услугам.

С 2010-х годов киберпреступность стала еще более изощренной: участились атаки на корпоративные сети, массовые утечки данных, мошенничество с криптовалютами и deepfake-технологиями.

Сегодня кибермошенничество - это глобальная проблема, затрагивающая миллионы людей по всему миру, а борьба с ним требует постоянного совершенствования законодательства и технологий защиты.

Ответственность за мошенничество определяется Уголовным кодексом Российской Федерации. Мошенничество - это хищение чужого имущества или приобретение права на него путём обмана или злоупотребления доверием. В Уголовный кодекс РФ включены 6 статей, содержащих ответственность за совершение мошенничества, а именно: мошенничество в сфере кредитования, мошенничество при получении выплат, мошенничество с использованием электронных средств платежа, мошенничество в сфере страхования, мошенничество в сфере компьютерной информации и простое

¹ Ройхка А. А. Зарождение киберпреступности и этапы её последующего генезиса: российский и зарубежный опыт // Молодой ученый. - 2025. - № 13 (564). - С. 130.

мошенничество ¹.

Современные технологии кардинально изменили природу и масштабы мошенничества, открыв новые возможности. Технологический прогресс преобразовал мошенничество из локальноограниченных схем в высокоорганизованную инфраструктуру. Технологии расширили возможности мошенничества, создавая новые сложные схемы и пути обхода закона. С введения в нашу повседневную жизнь доступного интернета, социальных сетей, приложений и т.д. начали появляться разнообразные схемы кибермошенничества, которые всегда совершенствуются.

Мошенничество с использованием информационных технологий по-другому называется кибермошенничеством и обладает своей уникальностью - оно наносит колоссальный ущерб не только гражданам, но и предприятиям ². Кибермошенничество — это преступная деятельность, осуществляемая через интернет и цифровые технологии с целью обмана людей, кражи их денег, персональных данных или конфиденциальной информации включая фишинг, финансовые пирамиды, взломы банковских систем и социальную инженерию. Оно использует различные методы психологического воздействия, технические уловки и социальную инженерию, чтобы заставить жертву добровольно передать мошенникам средства или доступ к своим аккаунтам.

Системы противодействия не успевают развиваться также быстро как технологии, это делает кибермошенничество особенно опасным и сложнодоказуемым преступным деянием. Мошенники практически первые узнают о новых информационных технологиях и поэтому, узнавая о них подробнее, пользуются этим и, обманывая людей, получают деньги или имущество, обращая в свою пользу ³.

¹ Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) // Собрание законодательства РФ. - 2023. - № 50. - Ст. 7854.

² Сульгина В. С., Мацкайлова Е. В. Кибермошенничество: виды, схемы, способы противодействия // Материалы XXV Международного конкурса научно-исследовательских и творческих работ учащихся «Старт в науке». - М., 2023. - С. 4.

³ Шишкина М. В., Латыпова Э. Ю. Мошенничество с использованием информационных технологий: современные вызовы и ответы // Научный лидер. - 2025. - №17 (218). - С. 240.

Влияние разработки новых технологий проявляется в пяти ключевых аспектах, каждый из которых значительно усиливает опасность и масштабы киберпреступности.

1. Глобализация и автоматизация атак

Благодаря цифровым инструментам мошенники получили возможность проводить массовые атаки с минимальными затратами. Автоматизированные системы рассылки позволяют одновременно охватывать десятки тысяч потенциальных жертв по всему миру, а использование облачных технологий и готовых преступных сервисов сводит к минимуму организационные расходы. Глобальный характер интернета стирает географические границы преступной деятельности, затрудняя международное сотрудничество правоохранительных органов.

2. Эволюция методов обмана

Современные технологии обеспечивают точность и изощренность мошеннических схем. Анализ больших данных и технологии направленной рекламы позволяют мошенникам выявлять наиболее уязвимые группы населения и адаптировать атаки под конкретные случаи.

Появление новых платформ, например мессенджеров, социальных сетей, систем мгновенных платежей - создает дополнительные возможности для воздействия на жертв.

3. Преодоление систем защиты

Киберпреступники активно используют новые технологии для обхода защитных механизмов. Машинное обучение помогает им разрабатывать сложные алгоритмы, способные обходить традиционные системы обнаружения подозрительных действий.

Важно отметить, что преступники быстро адаптируются к новым алгоритмам технологий, в основном обход новых методов защиты занимает не более 24-48 часов.

4. Совершенствование анонимности

Современные технологии обеспечивают злоумышленникам

практически полную безнаказанность. Криптовалюты и миксеры транзакций эффективно скрывают движение украденных средств. Технологии VPN, TOR и прокси-серверов затрудняют идентификацию реального местоположения.

Особую проблему представляет использование одноразовых цифровых идентификаторов и автоматизированных систем уничтожения улик, которые активируются при первых признаках опасности.

5. Психологическая манипуляция нового уровня

Современные мошенники превратили социальную инженерию в точную науку. Анализ цифрового следа жертвы в социальных сетях позволяет создавать персонализированные сценарии атак с высочайшей степенью достоверности.

Технологии эмоционального программирования, основанные на исследованиях поведенческой психологии, значительно повышают эффективность манипуляций. Особенно опасны комбинированные атаки, сочетающие фишинг, вишинг (голосовой фишинг) и смс-мошенничество, создающие эффект «критической ситуации», подавляющий рациональное мышление жертвы.

Новые технологии не просто модернизировали традиционные схемы мошенничества - они создали принципиально новую парадигму киберпреступности, характеризующуюся беспрецедентными масштабами, изощренностью методов и глобальным характером угрозы. Противодействие этим вызовам требует постоянного развития систем кибербезопасности, совершенствования законодательства и повышения цифровой грамотности населения.

1.2 Типы мошеннических схем в цифровую эпоху

Классические схемы, которые раньше имели популярность, например поддельные лотереи, устарели и на их замену пришел искусственный интеллект, deepfake, фишинг и т.д., эти и другие схемы разберем подробно.

1. Искусственный интеллект (ИИ) и deepfake ¹

Искусственный интеллект (ИИ) - это технология, способная анализировать данные, обучаться и принимать решения, имитируя человеческое мышление. Его разработка началась еще в 1956 году, но настоящий прорыв произошел лишь в последние десятилетия благодаря развитию вычислительных мощностей и алгоритмов машинного обучения ². Изначально ИИ создавался для решения сложных задач, автоматизации процессов и улучшения качества жизни, однако, как и многие другие технологии, он стал инструментом в руках мошенников.

Используя ИИ, мошенники создают «голосовые клоны» разных людей, в основном используются голоса близких и друзей жертвы или создают чат-бот с ИИ где имитируют живое общение (например данный чат может представляться как техподдержка) для того чтобы обманным путем получить денежные средства.

Благодаря популяризации искусственного интеллекта специалисты начали расширять его функции и способности, что дало возможность развитию разных схем мошенничества в том числе и deepfake.

Идея создания deepfake возникла в 1990 году, а сам термин появился в 2017 году, когда пользователь интернета начал публиковать видео, в которых лица знаменитостей были заменены на лица других людей ³.

С помощью ИИ мошенники создают поддельные фото и видео в которых используют настоящие фотографии родственников, друзей, самого пострадавшего или знаменитых людей для получения денег или шантажа.

2. Социальные сети ⁴

В современном цифровом мире социальные сети стали неотъемлемой

¹ Шалагин А. Е., Идиятуллов А. Д. Трансформация преступности в XXI веке: особенности предупреждения и противодействия // Вестник Казанского юридического института МВД России. - 2021. - Т. 12. - № 2(44). - С. 230.

² Дербичев С. Б. Применение современных технологий в расследовании мошенничества // Молодой ученый. - 2025. - № 11 (562). - С. 150.

³ Воронин И. А., Гавра Д. П. Дипфейки: современное понимание, подходы к определению, характеристики, проблемы и перспективы // Российская школа связей с общественностью. - 2024. - № 33. - С. 15.

⁴ Тимофеев А. В., Комолов А. А. Киберпреступность как социальная угроза и объект правового регулирования // Современные философские исследования. - 2021. - № 1. - С. 98.

частью повседневной жизни миллионов людей. Однако их популярность и доступность создают широкие возможности для преступных действий. Мошенники активно используют платформы социальных сетей для реализации различных схем обмана, пользуясь доверием пользователей.

Одним из распространенных методов является создание поддельных аккаунтов, где злоумышленники выдают себя за других людей. Это могут быть поддельные профили работодателей, предлагающих несуществующие вакансии, или романтических партнеров, вступающих в виртуальные отношения с целью последующего вымогательства. Постепенно завоевывая доверие жертвы, мошенники начинают просить денежные переводы, интимные фотографии или конфиденциальную личную информацию, которую затем используют для шантажа.

Еще одной из опасных схем является взлом реальных аккаунтов пользователей. При регистрации в социальных сетях человек создает уникальный пароль, который должен обеспечить защиту его личных данных. Однако мошенники используют различные методы для получения доступа к учетным записям: фишинговые ссылки, вредоносное ПО, подбор паролей или пользуются уязвимостями в системе безопасности. Получив доступ к аккаунту, злоумышленники в первую очередь пишут друзьям и родственникам владельца, которые, доверяя знакомому профилю, выполняют просьбы о денежных переводах на указанные реквизиты. Другой распространенной практикой является поиск и копирование личной информации из переписок и фотографий для последующего шантажа самого владельца аккаунта.

Особую опасность представляют случаи, когда мошенники используют несколько методов, создавая сложные многоуровневые схемы. Например, они могут сначала создать поддельный аккаунт, установить доверительные отношения, а затем попросить установить какое-либо приложение или перейти по ссылке, что в результате приводит к утечке личных данных или данных доступа к различным важным приложениям.

3.Криптовалюты или блокчейн- мошенничество

Мошенничество с использованием криптовалют представляет собой серьезную проблему, ставшую возможной благодаря развитию цифровых финансовых инструментов ¹.

Криптовалюта представляет собой цифровую форму денег, не имеющую физического выражения. В отличие от традиционных валют, она существует исключительно в виде данных - цепочек зашифрованной информации, защищённой криптографическими методами. Основой криптовалют является технология блокчейн - распределённый реестр, в котором хранится информация обо всех совершённых операциях.

Блокчейн состоит из последовательности блоков, каждый из которых содержит данные о транзакциях, а также криптографическую ссылку на предыдущий блок, что делает систему прозрачной и устойчивой к изменениям. Поскольку реестр хранится не в одном месте, а распределён между множеством участников сети, подделать или удалить записи практически невозможно.

Криптовалюты и блокчейн открыли новые перспективы для финансового мира: они позволяют проводить быстрые и относительно дешёвые международные переводы, обеспечивают анонимность (или псевдоанонимность) и снижают зависимость от банковских систем. Однако эти же особенности сделали их привлекательными для мошенников. В этой сфере созданы разные виды мошенничества, разберем некоторые из них:

3.1. Фишинговые атаки.

Фишинг относится к технологиям из сферы социальной инженерии, он опирается на факт незнания пользователем основ информационной безопасности ² . Целью фишинга является получения доступа к

¹ Вестов Ф. А., Абдрашитов А. Р. Возможности цифровых технологий по противодействию мошенничеству // Научный - практический журнал Базис. - 2024. - № 2 (16). - С. 26.

² Красовская Н. Р. К вопросу о кибермошенничестве // Вестник Удмуртского университета. Социология. Политология. Международные отношения. - 2022. - № 1. - С. 12.

конфиденциальной информации пользователей, в основном получение личных и платежные данные ¹.

В этом способе используется массовая рассылка электронных писем от имени популярных брендов или личных сообщений от различных серверов, например от имени банка. В письме указывается просьба «подтвердить кошелёк» или «обновить данные» и прямая ссылка на сайт, внешне не отличающегося от настоящего.

После того как пользователь попадает на поддельную страницу, ему предлагают ввести свои данные, например логин и пароль или данные банковского счета, затем преступник получает данные и использует их в своих целях. Реальные сервисы не рассылают письма с просьбами сообщить свои личные данные; такие письма и сообщения приходят только от кибермошенников ².

3.2. Мошенничество с NFT

Рост популярности онлайн-торговли на маркетплейсах привел к распространению нового вида мошенничества - созданию поддельных магазинов или объявлений, имитирующих известные торговые площадки. Злоумышленники создают копии реальных магазинов, используя схожие названия, логотипы и дизайн, чтобы ввести пользователей в заблуждение ³. Жертвы, полагая, что совершают покупку на официальном маркетплейсе, используют функцию быстрых платежей для оплаты товара, однако деньги поступают прямо на счет мошенников, а заказанные товары так и не приходят.

Такие схемы особенно опасны тем, что мошенники часто предлагают популярные или дефицитные товары по заниженным ценам, что привлекает больше потенциальных жертв. Кроме того, они могут использовать фишинговые ссылки, фальшивые отзывы и поддельные сертификаты

¹ Ширшиков А. С. Мошенничество как вид цифровой преступности // Молодой ученый. - 2022. - № 51 (446). - С. 592.

² Красовская Н. Р. Указ. соч.

³ Баймедетов С. Д., Пак Л. Ю. Тенденции финансового мошенничества в эпоху цифровизации // Вестник науки. - 2024. - 11 (80). - С. 62.

качества, чтобы усилить видимость легитимности. После получения платежа злоумышленники либо исчезают, либо затягивают сроки доставки под надуманными предлогами, а затем блокируют все контакты с покупателем.

3.3. Пирамиды и финансовые схемы

Одной из распространенных схем финансового мошенничества является создание фальшивых инвестиционных проектов с заведомо нереалистичными условиями. Преступники разрабатывают профессионально выглядящие сайты или платформы, предлагая вложения с огромной доходностью - 50-100% и выше, что в разы превышает стандартные рыночные показатели (например, ключевая ставка или доходность надежных активов редко превышает 5-15%)¹. Для привлечения жертв мошенники активно используют агрессивную рекламу в соцсетях, мессенджерах и на сайтах, публикуют фальшивые отзывы «успешных инвесторов» и создают видимость срочности: «Успейте вложиться до закрытия набора!».

После того как доверчивые пользователи переводят деньги, организаторы проекта какое-то время могут поддерживать иллюзию его работы: отправлять «отчеты» о росте инвестиций, выплачивать небольшие проценты (за счет средств новых вкладчиков) или даже имитировать торговую активность. Однако, как только приток новых средств снижается, мошенники исчезают, блокируя доступ к аккаунтам и сайтам, а все контакты обрываются.

Такие схемы, известные как финансовые пирамиды или скам-проекты, особенно опасны тем, что их создатели используют методы психологического давления - обещают «гарантированную прибыль», ссылаются на несуществующие лицензии или партнерства с известными компаниями. Жертвами часто становятся не только неопытные инвесторы, но и те, кто осознает риски, но надеется «успеть вывести деньги до краха».

Все эти виды связаны именно с кражей денежных средств или

¹ Наймушина К. М., Беляев А. П. Современное состояние киберпреступности: мошеннические схемы в сети интернет // Вестник науки. - 2024. - №5 (74). - том 3. - С. 479.

доступом к их месту хранения.

4. Мобильные приложения и вредоносные ПО

Мошенники активно используют вредоносное программное обеспечение для кражи денежных средств и конфиденциальных данных пользователей. Одним из распространенных методов является создание поддельных приложений, которые имитируют легальные сервисы - банковские программы, клиенты маркетплейсов, мессенджеры или даже государственные порталы. Такие приложения могут выглядеть практически идентично оригиналам, но при установке либо запрашивают избыточные разрешения, либо внедряют шпионские модули, перехватывающие логины, пароли, банковские реквизиты и SMS-коды подтверждения.

Еще один опасный способ атак - поддельные игры и пиратские версии популярных серверов. Пользователи, пытаясь скачать взломанную программу или игру бесплатно, вместо ожидаемого контента получают «троянские» программы, которые могут шифровать файлы с требованием выкупа, скрытно использовать криптовалюту или воровать данные для доступа к онлайн-аккаунтам. Особенно часто подобные схемы встречаются на сомнительных торрент-трекерах и файлообменниках.

Шпионские программы действуют еще тоньше - они могут длительное время оставаться незамеченными, собирая историю браузера, переписку, геолокацию и даже записывая нажатия клавиш. Полученные данные затем либо используются для прямого хищения средств, либо продаются в даркнете.

5. Социальная инженерия и мошенничество с помощью телефонных звонков.

Мошенники от имени банка или службы безопасности обзванивают людей под предлогом утечки данных или больших неизвестных переводов, предлагает варианты решения данной проблемы, при которых нужно предоставить паспортные данные или код подтверждения.

На сайте Центрального банка России опубликована диаграмма часто

используемых мошеннических схем. Впервые в пятерке популярных у кибермошенников приемов - получение доступа к аккаунтам людей на Госуслугах. Это свидетельствует о растущей активности злоумышленников, стремящихся завладеть персональными данными граждан для совершения финансовых махинаций или получения конфиденциальной информации. На остальные способы мошенничества (фишинговые ресурсы, поддельные QR- коды и прочие) пришлось 13,7% ¹.



Рис. 1 Диаграмма часто используемых мошеннических схем ²

Смотря на диаграмму, можно сделать вывод, что самой часто используемой схемой является телефонные звонки или СМС - сообщения. При этом, даже если они остаются главенствующими, они все равно изменились с развитием технологий. Все чаще телефонные звонки становятся deepfake- звонками использующие чужие голоса с приемами социальной инженерии.

¹ Кибермошенничество: портрет пострадавшего. - URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения: 29.03.2025).

² Там же.

1.3 Социальные последствия цифрового мошенничества

Цифровое мошенничество представляет собой серьезную социальную проблему, оказывающую комплексное негативное воздействие на различные сферы общественной жизни. Анализ последствий этого явления позволяет выделить несколько ключевых аспектов его влияния.

Одним из основных последствий является социальное неравенство. Каждый год миллионы людей становятся жертвами кражи личных данных и незаконного использования своих кредитных карт ¹. Жертвами мошенничества может стать любой человек, но наибольший интерес для них представляют граждане, которые часто используют банковские сервисы ².

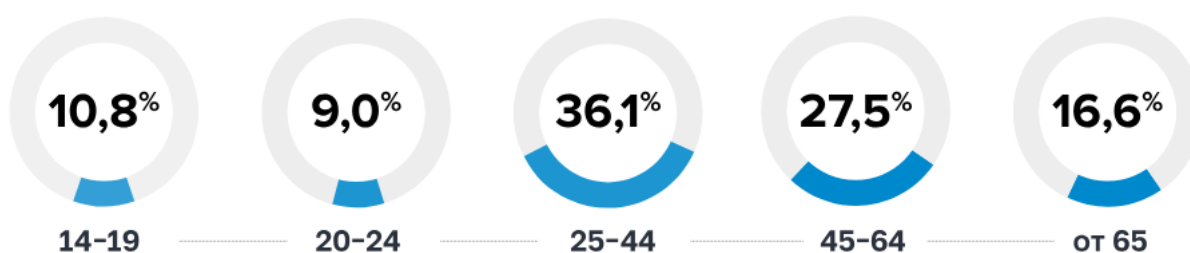


Рис.2 Процентное соотношение жертв по возрастным группам ³

В контексте социального неравенства наблюдается парадоксальная ситуация: хотя потенциальной жертвой может стать любой пользователь цифровых технологий, наиболее уязвимой группой оказываются экономически активные граждане в возрасте 25-64 лет, преимущественно со средним уровнем образования и дохода.

¹ Баубекова Ж., Носова Е. С., Кабанова Н. А. Мошенничество: социальное влияние и роль цифровых технологий в его распространения // Вестник евразийской науки. - 2024. - Т. 16. - С. 5.

² Кибермошенничество: портрет пострадавшего. - URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения: 29.03.2025).

³ Там же.



Рис 3. Уровень образования и достатка ¹

Эта закономерность, иллюстрируемая статистическими данными, объясняется сочетанием двух факторов - активным использованием финансовых сервисов и недостаточной цифровой грамотностью.

Социальное неравенство не является самым главным социальным последствием. В большей степени страдает экономика и доверие людей.

Люди используют сбережения, берут кредиты, попадают в долговую яму, что приводит к психологическому вреду. Бизнес-структуры несут значительные убытки от мошеннических схем, что влечет за собой сокращение рабочих мест и снижение инвестиционной привлекательности.

Жертвы мошенничества более эмоционально нестабильны по сравнению с теми, кто не стал жертвой ². Жертвы испытывают чувство вины, стыда, страх повторного обмана, что приводит к тому, что жертвы не обращаются в правоохранительные органы для возбуждения дел, виня в произошедшем себя и свою необразованность или неосведомленность, что создает «эффект темной цифры» в статистике преступлений.

Пропадает доверие к цифровым технологиям, люди перестают пользоваться привычными серверами (банки, госуслуги, социальные сети) из-за утечки данных. Распространение фобий, связанных с использованием онлайн-сервисов, приводит к добровольной цифровой изоляции наиболее уязвимых групп населения, т.к. растет подозрительность и усложняются

¹ Кибермошенничество: портрет пострадавшего. - URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения: 29.03.2025).

² Данилова Е. П., Портняга Е. М. Финансовое мошенничество в современном мире // SiberianSocium. - 2023. - Том 7. - № 2 (24). - С. 85.

социальные взаимодействия. Это, в свою очередь, усугубляет социальное неравенство и снижает эффективность цифровизации государственных услуг.

Психологические последствия носят долгосрочный характер: у пострадавших развивается хроническая тревожность, паранойя, нарушаются социальные связи. Следует отметить и инновационные риски: гиперосторожность пользователей и бизнеса замедляет внедрение перспективных цифровых технологий. Компании теряют потенциальных клиентов, инвесторы становятся более осторожными, что в конечном итоге тормозит развитие цифровой экономики.

Государство вынуждено увеличивать расходы на кибербезопасность, одновременно балансируя между необходимостью защиты граждан и сохранением цифровых свобод.

Мошенничество в целях манипуляции гражданами (например, перед выборами), теории о постоянной слежке через камеры устройств или прослушивание телефонных разговоров дестабилизирует общество и подрывает доверие к государству и закону.

Цифровое мошенничество трансформируется из чисто криминальной проблемы в комплексный социальный феномен, требующий междисциплинарного подхода к решению. Его последствия выходят далеко за рамки материального ущерба, затрагивая основы социального взаимодействия и доверия в цифровую эпоху.

2 Анализ и противодействие мошенничеству

2.1 Анализ реальных случаев мошенничества в Пензенской области

Мошенники перешли из реальной жизни в виртуальную, так как компьютерные сети предоставляют им безопасность, анонимность, и возможность совершать массовые атаки на людей.

С января по декабрь 2024 года в Российской Федерации зарегистрировали 765,4 тыс. киберпреступлений, что на 13,1% больше, чем за аналогичный период 2023 года. В общей сложности от рук кибермошенников в 2024 году пострадали 448,9 тыс. человек ¹.

В 2024 г. на территории Пензенской области отмечается рост киберпреступности. В регионе зарегистрировано 6 916 противоправных деяний, совершенных с использованием сотовых средств связи и сети «Интернет». В видах преступлений преобладают мошенничества (41 %) и неправомерный доступ к охраняемой законом компьютерной информации (33 %) ². Большое число мошенничества происходило в Пензе, Кузнецке и Лунинском районе. 80% от общего количества мошенничеств в Пензенской области совершались в интернете, мессенджерах и с использованием сотовых телефонов.

Прокуратура следила за тем, чтобы пострадавшим вернули украденные деньги. На этапе следствия уже возмещено 16 миллионов рублей, еще на 9 миллионов наложен арест на имущество подозреваемых ³.

¹ Кабанов П. А. Жертвы кибермошенничества как один из объектов современной кибервиктимологии: краткий статистический анализ показателей криминальной виктимности 2021 - 2022 гг. // Виктимология. - 2023. - Т. 10. - № 1. - С. 20.

² Органы прокуратуры области принимают меры по защите прав потерпевших по уголовным делам о телефонных мошенничествах. - URL: https://epp.genproc.gov.ru/web/proc_58/mass-media/news?item=100258785 (дата обращения: 05.04.2025).

³ Жители Пензенской области за год перечислили мошенникам более 1 млрд рублей. - URL: <https://penzavzglyad.ru/news/176923/zhiteli-penzenskoy-oblasti-za-god-perechislili-moshennikam-bolee-1-mlr-rublej>(<https://penzavzglyad.ru/news/176923/zhiteli-penzenskoy-oblasti-za-god-perechislili-moshennikam-bolee-1-mlr-rublej>) (дата обращения: 05.04.2025).

Разберем несколько реальных случаев мошенничества в Пензенской области за период 2021 - 2025 года. В связи с отсутствием доступной судебной практики по кибермошенничеству в Пензенской области, информация была взята из региональных новостных порталов и форумов.

Одним из случаев в 2021 году стало мошенничество под видом инвестиционной компании «Финико». Организаторы привлекали людей через прямые эфиры в соцсетях и проводили конференции в разных городах, где убеждали аудиторию в возможности «зарабатывать в кризис» и покупать недвижимость за 30% от рыночной стоимости. Как минимум трое жителей Пензенской области перевели через интернет-платформу компании более 845 тысяч рублей, после чего мошенники исчезли. По факту обращения пострадавших было возбуждено уголовное дело по ч. 3 и ч. 4 ст. 159 УК РФ (мошенничество в особо крупном размере).

В 2022 году пенсионерка из Пензы получила звонок от человека, представившегося сотрудником Центрального банка. Мошенник сообщил, что на ее имя пытаются оформить кредит, и для «защиты средств» предложил самостоятельно взять заем и перевести деньги на «безопасный счет». Женщина оформила кредит на 300 тысяч рублей и перевела их злоумышленникам. Осознав обман, она обратилась в полицию, и было возбуждено дело по ч. 3 ст. 159 УК РФ.

В 2023 году в Пензе несколько человек стали жертвами мошенников, которые использовали поддельное мобильное приложение, сложно отличимый от оригинального приложения интернет-банк. Жертвы, поверив в подлинность программы, вводили свои данные, после чего с их счетов было похищено в общей сложности 1,2 миллиона рублей. По факту хищения возбуждено уголовное дело.

В 2024 году жительницу Заречного обманули с помощью технологии deerfake - ей позвонил мошенник, использовавший поддельный голос ее дочери. Злоумышленник сообщил о «чрезвычайной ситуации» и попросил срочно перевести денежные средства по данному номеру телефона. Женщина

перевела 1,2 миллиона рублей, прежде чем поняла, что стала жертвой мошенничества.

В начале 2025 года 19-летняя жительница Пензы познакомилась в сети с молодым человеком, и их виртуальные отношения развивались до момента, когда она отправила ему интимные фото. После этого под угрозой распространения снимков он требовал деньги. Девушка перевела шантажисту 70 тысяч рублей, но требования не прекратились. Осознав, что выплаты будут бесконечными, она обратилась в полицию. обратилась в полицию, где было возбуждено уголовное дело по статье за вымогательство.

Эти случаи - лишь небольшая часть мошеннических схем, с которыми сталкиваются жители Пензенской области. Преступники постоянно совершенствуют методы: используют фейковые инвестиции, сочинженерию, поддельные приложения и искусственный интеллект. К сожалению, значительная часть пострадавших от действий мошенников предпочитает не обращаться в правоохранительные органы. из-за стыда или неверия в возврат денег, что позволяет мошенникам оставаться безнаказанными. Однако это лишь усугубляет проблему. Отсутствие официальных заявлений мешает правоохранительным органам выявлять схемы мошенников, отслеживать их активность и привлекать злоумышленников к ответственности. В результате преступники продолжают безнаказанно действовать, находя новых жертв.

2.2 Расследование кибермошенничества

Расследование кибермошенничества представляет собой сложный многоэтапный процесс, требующий комплексного подхода и взаимодействия различных структур ¹. Эффективность расследования кибермошенничества во многом зависит от профессиональной подготовки специалистов, технического оснащения правоохранительных органов и степени

¹ Маилян А. В. Актуальные вопросы расследования и раскрытия кибермошенничества «фишинг» // Философия права. - 2022. - № 2 (101). - С. 113.

межведомственной координации.

На сегодняшний день анализ практики и статистических данных свидетельствует о том, что только 23% случаев кибермошенничества завершаются полным возвратом средств, что подчеркивает важность грамотного подхода на всех этапах. Успех зависит от скорости реакции, качества собранных доказательств и грамотного взаимодействия со всеми участниками процесса.

Первое, что нужно сделать, незамедлительно зафиксировать факт обмана и собрать все возможные доказательства. Чем быстрее это сделать, тем больше шансов найти преступников и вернуть деньги. Успех расследования кибермошенничества во многом предопределяется количеством и качеством оперативно-розыскной информации, полученной ещё до возбуждения уголовного дела ¹. На этой стадии крайне важно обеспечить сохранность цифровых доказательств, а именно:

- Детали мошеннической схемы (как именно произошёл обман - фишинг, поддельный магазин, взлом аккаунта, социальная инженерия т.д.).
- Финансовые операции (реквизиты получателя, номера карт, криптовалютные кошельки, скриншоты переводов).
- Цифровые следы (переписки в мессенджерах, электронные письма, история браузера).
- Технические данные (если было заражение вирусом - файлы вредоносного ПО, IP-адреса атакующих).

Чем больше доказательств собрать, тем проще будет правоохранительным органам найти мошенников.

После этого нужно сразу обратиться в полицию и банк (если деньги успели перевести), чем быстрее подано заявление, тем выше вероятность блокировки переводов и поимки преступников. Важным аспектом расследования является взаимодействие с финансовыми учреждениями. Банки и платежные системы играют ключевую роль в оперативном

¹ Билан А. Н. Методика расследования кибермошенничества // Молодой ученый. - 2022. - № 32 (427). - С. 67.

блокировании подозрительных транзакций и предоставлении информации о денежных потоках. В последние годы отмечается тенденция к автоматизации данного процесса через системы мониторинга, работающие в режиме реального времени.

После сбора всех данных о мошенничестве (чеки, переписки, номера карт и т. д.), начинается этап поиска злоумышленников: техническая часть расследования ¹:

- Трассировка платежей:

Если деньги ушли на банковскую карту, необходимо немедленно обратиться в банк с заявлением о мошенничестве. Банк может заблокировать перевод, если он еще не прошел.

Особую сложность представляет расследование преступлений, связанных с использованием криптовалют. В таких случаях применяются специализированные методы блокчейн-анализа, позволяющие отследить движение средств через цепочку транзакций. Специалисты могут выявить биржи, через которые обналичиваются деньги, и подать запрос на заморозку средств.

- Анализ контактов мошенников:

Номера телефонов проверяются через базы данных (например, «Антифрод» или сервисы анализа мошеннических схем).

Электронные адреса исследуются через WHOIS, поиск утечек данных и связей с другими преступлениями.

Аккаунты в соцсетях и мессенджерах (Telegram, WhatsApp, Viber) могут помочь установить личность злоумышленника.

- Киберкриминалистика (если использовалось вредоносное ПО):

Анализ кода вируса (трояны, шифровальщики) помогает выявить серверы управления и возможных заказчиков атаки. Исследуются сетевая активности для определения IP-адресов и геолокации злоумышленников.

Особую сложность представляет идентификация злоумышленников,

¹ Маилян А. В. Указ. соч.

использующих современные методы анонимности. Если мошенники действовали не через полностью анонимные сервисы, их можно попытаться вычислить. Вот основные способы, которые используют правоохранительные органы и специалисты по кибербезопасности:

- По IP-адресу (запрос к интернет-провайдеру, но часто злоумышленники используют VPN или прокси) ¹.

- Через привязку телефона/почты (если они не использовали одноразовые номера).

- По банковским реквизитам (если деньги ушли на карту, банк раскроет данные владельца по запросу правоохранительных органов).

- Через цепочку транзакций (особенно в криптовалютах - если преступники выводили деньги на биржи, их можно идентифицировать).

Заключительный этап расследования предполагает подготовку материалов для судебного разбирательства. Особое внимание уделяется правильному оформлению цифровых доказательств, их надлежащему хранению и представлению в суде.

Международное сотрудничество является неотъемлемой частью расследования киберпреступлений. Практика показывает, что большинство сложных схем мошенничества имеют трансграничный характер ².

Эффективное противодействие таким угрозам требует выстроенной системы международного взаимодействия, которая включает несколько уровней. На институциональном уровне ключевую роль играют такие организации как Интерпол, создавший Глобальный комплекс по борьбе с киберпреступностью (IGCI), и Европол с его Европейским центром по борьбе с киберпреступностью (EC3). Эти структуры обеспечивают координацию между национальными правоохранительными органами, проводят

¹ Баишев Д. А. Особенности расследования кибермошенничества // Молодой ученый. - 2025. - № 20 (571). - С. 376.

² Клевцов К. К. Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам // Вестник Санкт-Петербургского университета. - 2022. - Т. 13. - Вып. 3. - С. 680.

совместные операции и организуют обмен лучшими практиками ¹.

В целях улучшения международного сотрудничества связанного с киберпреступностью 24 декабря 2024 года Генеральная Ассамблея ООН консенсусом одобрила Конвенцию против киберпреступности (полное название - «Конвенция против киберпреступности; Укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям») ².

Документ разработан по инициативе России и стал первым в истории универсальным международным договором в области информационной безопасности.

Цель конвенции - стать основой для налаживания правоохранительного сотрудничества в противодействии использованию информационно-коммуникационных технологий (ИКТ) в преступных целях.

В соответствии со статьёй 35 Будапештской конвенции о киберпреступности была создана сеть контактов- Сеть 24/7 ³.

Цель сети - обеспечить оперативную помощь странам-участницам конвенции при расследованиях и судебных разбирательствах, связанных с уголовными преступлениями, связанными с компьютерными системами и данными, или для сбора доказательств в электронной форме ⁴.

Большинство контактных пунктов сети 24/7 прикреплены к специализированным полицейским или прокурорским службам по борьбе с киберпреступностью. Эти центры, функционирующие круглосуточно, позволяют оперативно запрашивать и получать электронные доказательства

¹ Клевцов К. К. Указ. соч.

² Конвенция против киберпреступности укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (принята резолюцией 79/243 Генеральной Ассамблеи ООН от 24.12.2024) / Официальный сайт ООН. - URL: <https://www.un.org/ru/?ysclid=mb0kd0afjo493654797> (дата обращения: 3.04.2025).

³ Конвенция о киберпреступности (ETS № 185) / Заключена в Будапеште 23.11.2001, для России вступила в силу 01.12.2021 // Бюллетень международных договоров. - 2021. - № 12. - С. 45.

⁴ The 24/7 Network established under the Convention on Cybercrime (known as the Budapest Convention) / Council of Europe 2016. - URL: <https://www.coe.int/en/web/cybercrime/24/7-network-new> (дата обращения: 05.04.2025).

из других стран, что, критически важно учитывая скорость, с которой могут быть уничтожены цифровые следы. В 2023 году через эту систему было обработано более 15 тысяч запросов о правовой помощи.

Из вышеперечисленного можно сказать, что эффективность расследования зависит от трех основных факторов: скорости, подробности собранной информации и сотрудничестве между участниками. Расследование кибермошенничества требует оперативности и грамотного подхода, но важно понимать, что не все случаи удастся раскрыть быстро, особенно если злоумышленники работают из-за границы. Чтобы было больше шансов на раскрытие и возврат денег нужно действовать без промедления.

2.3 Методы противодействия новым технологиям в мошенничестве

Борьба с киберпреступностью осложняется целым рядом факторов:

1. Киберпреступники - это не обычные мошенники, а хорошо обученные программисты, которые скрываются за экраном своего компьютера. Такую личность вычислить гораздо сложнее, чем обычного преступника ¹.

2. Сотрудники правоохранительных органов нуждаются в помощи высококвалифицированных специалистов в сфере программирования.

3. Немало трудностей возникает и с определением самого факта совершения данного преступления. Ввиду отсутствия возможности проведения квалифицированной экспертизы, зачастую бывает сложно доказать, что за то или иное действие предусмотрено наказание ².

4. Достаточно трудно осуществлять контроль за уже существующими, постоянно обновляющимися и вновь возникающими видами киберпреступности.

¹ Тимофеев А. В. Указ. соч.

² Волынская О. В. Развитие юридической мысли и перспективы в борьбе с киберпреступностью в сфере уголовного судопроизводства // Вестник Московского университета МВД России. - 2020. - № 3. - С. 72.

Для противодействия новым цифровым технологиям необходимы современные методы защиты. С каждым годом наблюдается рост киберпреступности, которая подрывает экономику страны и дестабилизируют общество. Для минимизации рисков и повышения доверия людей многие специалисты из разных сфер создают технологии противодействующие киберпреступности.

В банковской сфере выделяют несколько вариантов противодействия кибермошенникам.

Во-первых можно выделить такой способ как искусственный интеллект. Хотя некоторые его и используют для мошенничества, он также может быть защитой для клиентов банка.

Главным преимуществом ИИ является его способность к быстрому обучению и адаптации. Эти технологии анализируют большое количество информации и выявляют действия похожие на мошеннические ¹. Они могут адаптироваться к новым схемам мошенничества, это ускоряет процесс обнаружения и противодействия. В данном случае ИИ становится более эффективен, чем традиционные методы.

Многие банковские системы уже начали вводить в эксплуатацию ИИ для предотвращения преступлений и минимизации риска, но для улучшения функций необходимо дальнейшее развитие технологий и алгоритмов.

Во- вторых использование биометрических технологий. Такой способ противодействия может стать более эффективным, т.к. биометрические данные практически невозможно подделать.

Банковские системы и приложения используют такие биометрические данные как:

1. Сканирование отпечатков пальца;
2. Распознавание лица;
3. Распознавание голоса.

Эти данные являются самыми популярными и уже используются в

¹ Дербичев С. Б. Указ. соч.

различных приложениях. Однако такой способ требует особого внимания к конфиденциальности данных пользователя. Необходимо дополнительно разрабатывать алгоритмы для гарантии защиты биометрической информации.

В будущем ожидается, что биометрические технологии будут взаимодействовать с ИИ для создания многоуровневой защиты, что повысит эффективность этого способа.

В- третьих использование аутентификации пользователей. Данный способ уже давно используется и улучшается.

Кроме парольной аутентификации, где можно подтвердить свою личность одним паролем, ввели двухфакторную, т.е. использование двух различных способов для подтверждения личности и получения доступа к данным банковского счета. В таком случае чаще всего используют сначала пароль, затем код из СМС сообщений.

Все эти способы также используются в различных приложениях и социальных сетях.

Способы кибермошенничества различны, и связаны не только банковской сферой. Борьба со многими схемами человеку приходится самостоятельно. Разберем несколько способов противодействия другим способам.

1. Клонирование голоса.

В таком мошенничестве сложно определить подлинность голоса, иногда это не под силу даже экспертам.

Для противодействия такой схеме лучшим вариантом будет спокойствие и подозрительность. При получении звонка или сообщения с неизвестных номеров от имени близких, нужно связаться с ними с помощью привычных способов общения и подтвердить или опровергнуть данную мошенником информацию.

2. Фишинг и спам по электронной почте.

Данные письма с первого взгляда выглядят правдоподобными, но

скрывают в себе угрозу для данным.

Если нет уверенности в действительности данного письма и в личности отправителя не нужно открывать ссылки или файлы, прилагаемые к данному письму.

3. Социальные сети.

Используя, личные данные мошенники используют аккаунты пользователей сети. Для минимизации рисков желательно использовать многофакторную систему аутентификации, для быстрого получения сведений о подозрительных активностях.

Из- за использования чужих аккаунтов мошенниками в небезопасном положения находятся не только владельцы, но и их близкие.

Для предотвращения мошеннических схем близким рекомендуется игнорировать сообщения или связаться с владельцем другим доступным способом.

4. Deepfake и шантаж.

С помощью искусственного интеллекта возможно создать фото или видео с лицом жертвы, которые порочат честь и достоинство. Данный способ используется для шантажа и вымогательства денежных средств. Такой схеме сложно противодействовать из- за социального мнения и других факторов, которые волнуют пострадавшего.

При этом вместо выполнения требований шантажиста лучше всего обратиться в правоохранительные органы для возбуждения уголовного дела и сообщить большему числу знакомых о поддельных фотографиях или видео.

Каждому способу кибермошенничества можно противостоять самостоятельно или с помощью подходящих алгоритмов. Для граждан главный способ противодействия это спокойствие и рассудительность при возникновении таких ситуаций.

2.4 Роль государственного регулирования в борьбе с мошенничеством

Для борьбы с киберпреступностью, которая будет расти параллельно с дальнейшим развитием сферы использования информационных технологий, представляющей все большие возможности для противоправной деятельности как отдельным лицам, так и преступным группам, государственное регулирование играет ключевую роль в борьбе с мошенничеством, обеспечивая правовые, экономические и организационные механизмы для предотвращения, выявления и наказания злоумышленников ¹.

Основные направления государственного регулирования в борьбе с мошенничеством:

1. Законодательная база.

- Разработка и усовершенствование закона, криминализирующих мошенничество;
- Ужесточение санкций за финансовые махинации, кибермошенничество, корпоративное мошенничество;
- Регулирование сфер, особо подверженных мошенничеству (банковская сфера, страхование, госзакупки, криптовалюты).

Так 1 апреля 2025 года президентом был подписан закон о борьбе с кибермошенничеством. Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» внес изменения в несколько федеральных законов (например, закон ФЗ «О банках и банковской деятельности», «О защите прав потребителей», ФЗ «О федеральной службе

¹ Мартьянов Н. Р. Уголовно - правовая борьба с киберпреступлениями на современном этапе // Государственная служба и кадры. - 2020. - № 1. - С. 175.

безопасности», ФЗ «Об оперативно-розыскной деятельности» и т.д.)¹.

Данный ФЗ официально вступит в силу с 1 июня 2025 года, за исключением положений, для которых установлены иные сроки.

Разберем основные изменения:

1. Банки будут следить за выдачей наличных средств, т.е. добровольно ли клиент снимает деньги или под влиянием мошенников.

При наличии признаков, что клиент действует не по своей воле, банк будет ограничивать сумму снятия наличных, максимум 50 000 руб. в сутки.

Если информация о клиенте или карте внесена в базу данных ЦБ РФ о мошеннических действиях, банк ограничит выдачу наличных до 100 000 Р в месяц.

Физические лица или выбранное доверенное лицо будут подтверждать все или несколько операций по карте. Если транзакция не будет подтверждена, банк откажет ее проводить.

Данное изменения вступит в силу с 1 сентября 2025 г.

2. Банки, госорганы и компании с госучастием не могут передавать персональные данные и платежные документы через иностранные мессенджеры из перечня Роскомнадзора (например Telegram, WhatsApp, Viber) 1 июня 2025 г. к этому списку добавят новые мессенджеры.

3. Микрофинансовые организации, имеющие возможность заключать договор микрозайма онлайн, заключают договор после регистрации через госуслуги, после вступления закона в силу (официальное вступление 1 марта 2026 года) заключить договор онлайн можно будет только по биометрическим данным.

4. Абоненты мобильных операторов смогут отказаться от массовой рассылки рекламы, массовых и автоматических звонков.

Также оператор должен будет сообщить абоненту данные о том, кто звонит, если вызов совершает компания или ИП.

¹ О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 01.04.2025 № 41- ФЗ // Собрание законодательства РФ. - 2025. - № 14. - Ст. 1.

Физические лица смогут установить запрет на заключение договора с операторами через госуслуги или МФЦ. Для того чтобы убрать запрет нужно будет лично прийти в МФЦ и дать согласие на возможность заключение таких договоров.

Операторы связи перед заключением договора должны будут проверять количество сим- карт абонента и установлен ли запрет.

Абоненты смогут отказываться от рассылок с 1 августа 2025 г., от массовых и автоматических вызовов - с 1 сентября. Маркировка входящих звонков и возможность запрета заключения договора через госуслуги или МФЦ будет возможны с 1 сентября 2025 г.

Вышеперечисленные изменения минимизируют возможность кибермошенничества и улучшают работу важных серверов.

2. Надзор и контроль.

- Улучшение деятельности правоохранительных органов (МВД, Следственный комитет, ФСБ) по расследованию мошеннических схем;
- Модернизация работы финансовых регуляторов (ЦБ РФ, Росфинмониторинг) по выявлению теневых операций;
- Совершенствование контроля за рекламой и продажами (ФАС, Роспотребнадзор) для предотвращения обмана потребителей.

Специальная уголовно-правовая профилактика осуществляется в виде ведомственных и межведомственных программ, направленных на повышение уровня борьбы с преступностью, которые предполагает определенную систему мероприятий, направленных на осуществление профилактики конкретных видов преступлений, а также преступлений, совершенных на определенной территории и на профилактику преступности в общем ¹.

3. Международное сотрудничество.

- Участие в международных антикоррупционных и антимошеннических инициативах (G20, FATF);

¹ Майор А. А. Система мер противодействия мошенничеству и его распространению в российской федерации // Вестник науки. - Т.2. - 2020. - № 7 (28). - С. 73.

- Экстрадиция преступников и возврат похищенных активов.

4. Просвещение и профилактика.

- Информирование граждан о распространённых схемах обмана;

- Обучение сотрудников госструктур и бизнеса методам противодействия мошенничеству.

В условиях роста киберпреступности и сложных финансовых инструментов роль госрегулирования только возрастает, требуя постоянного улучшения мер борьбы с различными схемами кибермошенничества.

Обеспечение деятельности, направленной на противодействие распространению, как преступности в целом, так и мошенничеству, в качестве отдельно взятого состава преступления, является одной из наиболее приоритетных задач по снижению уровня преступности на территории Российской Федерации, так как выступает в качестве превентивной меры, которая предотвращает не только наступление общественно опасных последствий, но и совершение преступления в целом ¹.

¹ Майор А.А. Указ. соч.

3 Образование и безопасность

3.1 Образование и осведомленность населения

Предпосылкой возникновения такого негативного явления в обществе является, с одной стороны, всеобщая цифровизация, а с другой стороны - низкий уровень компьютерной и финансовой грамотности ¹.

Для того чтобы обезопасить граждан от кибермошеннических схем необходимо комплексное обучение распознаванию угроз и методам противодействия. Ключевое значение имеет разработка многоуровневой системы просвещения, адаптированной под разные возрастные и социальные группы. Для этого важно повысить возможности и эффективность распространения информации о кибермошеннических схемах.

1. Образовательные программы

Для молодых граждан эффективнее будет ввести в школах и вузах уроки цифровой грамотности, например, в рамках ОБЖ или информатики, либо ввести отдельное занятие, связанное именно с киберпреступлениями и способами противодействия. На таких занятиях можно разбирать реальные случаи мошенничества по разным схемам и объяснять пути распознавания угроз и действия которые нужны если уже произошел обман.

Такой подход позволит сформировать у учащихся критическое мышление и навыки безопасного поведения в цифровой среде. Это поможет школьникам и студентам обезопасить себя и своих близких. Зная, как работают мошенники и мошеннические схемы снизятся риски и уменьшится процент совершенных киберпреступлений.

Для пожилых людей создать бесплатные курсы как пользоваться приложениями и как защищать свои данные. Вывешивать в местах частого посещения пожилыми людьми (поликлиниках, МФЦ и т.д.) памятки с

¹ Намысов Е. Д. Мошенничество в цифровую эпоху в связи с общественными изменениями // Криминологический журнал. - 2023. - № 3. - С. 150.

простыми для понимания правилами безопасности.

Создания волонтерских программ, где молодые волонтеры будут обучать старшее поколение.

Для бизнеса и госучреждений ввести корпоративные тренинги по защите данных и фишингу. Регулярные проверки и тестовые рассылки для сотрудников, чтобы они учились распознавать и противодействовать мошенничеству на безопасных примерах.

2. Информационные компании

Распространение видов, схем, путей противодействия в СМИ и соцсетях. Публикования видеороликов с разбором схем (например «как распознать поддельный сайт банка»). Рассказывать истории жертв с анализом ошибок и проведения тестирования (определи, это мошенник или нет?)

Со стороны банка эффективнее будет оповещать своих клиентов о новых видах мошенничества в банковской сфере. Это можно производить с помощью СМС-сообщений или сообщений в приложении банка, баннеры на сайтах и в самом здании банка.

Со стороны государства можно использовать официальные сайты (например госуслуги) где будет размещаться актуальная информации о киберпреступности и способами противодействия. Также можно создать сайт или мобильное приложения, где будет возможно проверить на подлинность подозрительные ссылки.

Осведомленность населения - это фундамент цифровой безопасности. Системное обучение в сочетании с постоянным информированием позволит значительно снизить количество успешных мошеннических атак и создать культуру безопасного поведения в цифровой среде.

В этой связи Министерство труда и социальной защиты Российской Федерации совместно с Центральным Банком Российской Федерации проводит кампанию по повышению уровня финансовой киберграмотности

населения ¹. (Приложение)

3.2 Рекомендации по повышению мер безопасности

Распространение мобильного интернета, развитие системы ДБО и удалённых каналов предоставления финансовых услуг, рост доступности финансовых услуг для потребителей и другие факторы повышают вероятность подвергнуться рискам финансового мошенничества ².

В современных условиях цифровизации кибермошенничество становится одной из самых распространенных угроз, затрагивающих как частных лиц, так и организации. Для защиты от подобных рисков необходимо комплексно подходить к вопросам безопасности, начиная с базовых мер предосторожности.

Прежде всего, важно регулярно обновлять программное обеспечение и операционные системы, поскольку злоумышленники часто используют уязвимости устаревших версий.

Использование надежных и уникальных паролей для каждого аккаунта значительно снижает вероятность взлома, а двухфакторная аутентификация добавляет дополнительный уровень защиты.

Следует избегать перехода по подозрительным ссылкам в электронных письмах или сообщениях, особенно если они требуют ввода личных данных. Фишинговые атаки часто маскируются под официальные запросы от банков или сервисов, поэтому важно проверять отправителя и не раскрывать личную информацию³.

Обучение основам кибербезопасности всех пользователей интернета, включая сотрудников в организациях, помогает минимизировать риски, распознавать потенциальные угрозы и действовать осмотрительно.

¹ Кампания по повышению уровня финансовой киберграмотности населения. - URL: <https://disk.yandex.ru/d/ju-52sM455e19g> (дата обращения: 03.04.2025).

² Барсуков М. В. Влияние цифровой трансформации на уровень риска финансового мошенничества // Фундаментальные исследования. - 2022. - № 11. - С. 20.

³ Заварыкина Ю. В., Абрамова Е. М. Некоторые виды интернет мошенничеств и способы борьбы с ними // Оригинальные исследования. - 2020. - Т. 10. - №12. - С. 67.

Копирование данных, учет всех финансовых операций и быстрое реагирование на подозрительную активность позволяют предотвратить ущерб от мошеннических схем.

В случае использования общественных сетей Wi-Fi рекомендуется применять приложения для шифрования геопозиции и трафика (например VPN).

Также важно не публиковать личную информацию в открытом доступе, поскольку злоумышленники могут использовать ее для социальной инженерии.

Внедрение этих практик в повседневную деятельность существенно снижает риски стать жертвой кибермошенников.

Главное - критическое мышление и техническая защита. Мошенники постоянно придумывают новые схемы, поэтому важно быть осведомленным о мошенничестве и способах противодействия.

Особое внимание следует уделить вопросам безопасности детей, которые могут стать жертвой преступлений, совершаемых с использованием компьютерных технологий и сети Интернет. Это может быть как банальное вымогательство, так и совершение преступлений сексуального характера, склонение к суицидальному поведению ¹.

Чтобы обеспечить безопасность детей в цифровом пространстве, важно выработать четкие правила поведения. Прежде всего, приучите детей посещать только те сайты, которые вы одобрили, и объясните, почему это важно. Особое внимание уделите защите личной информации - ребенок должен советоваться с вами перед тем, как делиться в сети любыми персональными данными, будь то фотографии, адрес или номер телефона.

Также установите запрет на скачивание файлов, программ или игр без вашего разрешения, чтобы избежать заражения устройства вирусами или вредоносным ПО.

¹ Как не стать жертвой киберпреступлений. - URL: https://penza.sledcom.ru/Poleznaja_informacija/item/1165598/ (дата обращения: 03.04.2025).

Помогите детям распознавать и игнорировать спам, а также регулярно беседуйте с ними о том, что они узнают в интернете, с кем общаются в соцсетях и какие темы обсуждают. Если ребенок планирует встречу с кем-то, с кем познакомился онлайн, или хочет совершить покупку через интернет, он обязательно должен посоветоваться с вами. Обсудите с ним риски, связанные с азартными играми и финансовыми махинациями, и постоянно напоминайте, чем может обернуться разглашение личной информации.

Для дополнительной защиты используйте родительский контроль: установите программы, блокирующие доступ к опасным сайтам, и приложения, уведомляющие о попытках их посещения. Будьте внимательны к изменениям в поведении ребенка - если он стал замкнутым, тревожным или скрывает свои онлайн-контакты, это может сигнализировать о проблемах. Важно, чтобы дети знали: в случае оскорблений, угроз или других неприятных ситуаций в сети они всегда могут обратиться к вам за помощью и поддержкой.

Главное - сочетать технические средства защиты с доверительным общением. Так можно минимизировать риски и научить ребенка осознанно и безопасно пользоваться интернетом.

ЗАКЛЮЧЕНИЕ

Таким образом, нами была достигнута цель и решены поставленные задачи исследования. В данной работе рассмотрены ключевые аспекты кибермошенничества в контексте современных технологий, его последствий и методов противодействия.

Подведем основные итоги работы:

Кибермошенничество представляет собой одну из наиболее динамично развивающихся угроз в цифровую эпоху. Оно охватывает широкий спектр преступных схем, включая фишинг, использование искусственного интеллекта (deepfake), криптовалютные аферы, социальную инженерию и вредоносное ПО.

Технологический прогресс не только расширил возможности мошенников, но и усложнил их выявление и доказательство, что делает эту проблему особенно актуальной.

Современные мошеннические схемы характеризуются:

1. Высокой степенью автоматизации и масштабируемости
2. Использованием передовых технологий (ИИ, блокчейн, нейросети)
3. Транснациональным характером деятельности
4. Усложненными механизмами отмывания денежных средств
5. Персонализацией атак на основе анализа больших данных

Особую тревогу вызывает растущая изощренность методов социальной инженерии. Как показало исследование, современные мошенники активно используют:

1. Психологические триггеры (эффект срочности, авторитетность)
2. Технологии глубокого обучения для анализа поведения жертв
3. Синтетические медиа (deepfake аудио и видео)
4. Мультиканальные схемы воздействия

Статистика показывает устойчивый рост киберпреступлений, что

негативно сказывается на экономике и общественной стабильности. Основными жертвами становятся экономически активные граждане в возрасте 25-64 лет.

Экономические последствия кибермошенничества носят системный характер. Помимо прямых финансовых потерь (которые только по официальным данным превышают несколько триллионов рублей ежегодно), наблюдаются:

1. Снижение доверия к цифровым сервисам
2. Замедление темпов цифровизации
3. Рост затрат на кибербезопасность
4. Потеря репутационного капитала компаний

Что подчеркивает необходимость целенаправленных мер защиты для этой группы.

Для эффективного противодействия кибермошенническим схемам требуется комплексный подход: повышение осведомленности о современных схемах мошенничества и методах защиты, создание современных алгоритмов и инструментов для выявления и предотвращения угроз, усиление правовых и организационных механизмов борьбы с киберпреступностью, спокойствие и рассудительность при взаимодействии с мошенническими схемами в цифровой среде.

Несмотря на рост числа таких преступлений, их раскрываемость остается низкой из-за технической сложности и транснационального характера.

Расследование кибермошенничества представляет собой сложный многоэтапный процесс, требующий слаженного взаимодействия потерпевших, правоохранительных органов, IT-специалистов, финансовых учреждений и международных организаций.

Ключевыми факторами успеха являются оперативность, качество собранных доказательств и координация между участниками процесса.

Данное исследование демонстрирует, что борьба с

кибермошенничеством требует комплексного подхода, соединяющее технологические решения, законодательные меры и активное вовлечение общества. Только совместными усилиями государства, бизнеса и граждан можно минимизировать риски и создать более безопасную цифровую среду.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно-правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Российская газета. - № 237. - 25.12.1993.

2. Конвенция о киберпреступности (ETS № 185) / Заключена в Будапеште 23.11.2001, для России вступила в силу 01.12.2021 // Бюллетень международных договоров. - 2021. - № 12. - С. 45-52.

3. Конвенция против киберпреступности укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (принята резолюцией 79/243 Генеральной Ассамблеи ООН от 24.12.2024) / Официальный сайт ООН. - URL: <https://www.un.org/ru/?ysclid=mb0kd0afjo493654797> (дата обращения: 3.04.2025).

4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) // Собрание законодательства РФ. - 2023. - № 50. - Ст. 7854.

5. О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 01.04.2025 № 41-ФЗ // Собрание законодательства РФ. - 2025. - № 14 - Ст. 1.

Публикации в научных журналах, сборниках и СМИ

6. Антонян Е. А. Блокчейн - технологии в противодействии кибертерроризму / Е. А. Антонян, И. И. Аминов // Актуальные проблемы российского права. - 2019. - № 6 (103). - С. 170 - 175.

7. Баймедетов С. Д. Тенденции финансового мошенничества в эпоху цифровизации / С. Д. Баймедетов, Л. Ю. Пак // Вестник науки. - 2024. - 11 (80). - С. 60 - 64.
8. Барсуков М. В. Влияние цифровой трансформации на уровень риска финансового мошенничества / М. В. Барсуков // Фундаментальные исследования. - 2022. - № 11. - С. 18 - 23.
9. Баубекова Ж. Мошенничество: социальное влияние и роль цифровых технологий в его распространения / Ж. Баубекова, Е. С. Носова, Н. А. Кабанова // Вестник евразийской науки. - 2024. - Т. 16. - С. 1 - 9.
10. Баишев Д. А. Особенности расследования кибермошенничества / Д. А. Баишев // Молодой ученый. - 2025. - № 20 (571). - С. 375 - 378.
11. Билан А. Н. Методика расследования кибермошенничества / А. Н. Билан // Молодой ученый. - 2022. - № 32 (427). - С. 65-68.
12. Воронин И. А. Дипфейки: современное понимание, подходы к определению, характеристики, проблемы и перспективы / И. А. Воронин, Д. П. Гавра // Российская школа связей с общественностью. - 2024. - № 33. - С. 1-20.
13. Вестов Ф. А. Проблемы противодействия киберпреступности, как основа повышения эффективности экономики / Ф. А. Вестов, П. П. Шмелев // Эксперт: теория и практика. - 2021. - № 2 (11). - С. 73- 76.
14. Вестов Ф. А. Возможности цифровых технологий по противодействию мошенничеству / Ф. А. Вестов, А. Р. Абдрашитов // Научный - практический журнал Базис. - 2024. - № 2 (16). - С. 25- 28.
15. Волынская О. В. Развитие юридической мысли и перспективы в борьбе с киберпреступностью в сфере уголовного судопроизводства / О. В. Волынская // Вестник Московского университета МВД России. - 2020. - № 3. - С. 72 -74.
16. Данилова Е. П. Финансовое мошенничество в современном мире / Е. П. Данилова, Е. М. Портняга // SiberianSocium. - 2023. - Том 7. - № 2 (24). - С. 67- 97.

17. Дербичев С. Б. Применение современных технологий в расследовании мошенничества / С. Б. Дербичев // Молодой ученый. - 2025. - № 11 (562). - С. 149- 152.
18. Заварыкина Ю. В. Некоторые виды интернет мошенничеств и способы борьбы с ними / Ю. В. Заварыкина, Е. М. Абрамова // Оригинальные исследования. - 2020. - Т. 10. - № 12. - С. 64- 71.
19. Клевцов К. К. Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам / К. К. Клевцов // Вестник Санкт-Петербургского университета. - 2022. - Т. 13. - Вып. 3. - С. 678-691.
20. Красовская Н. Р. К вопросу о кибермошенничестве / Н. Р. Красовская // Вестник Удмуртского университета. Социология. Политология. Международные отношения. - 2022. - № 1. - С. 12.
21. Кабанов П. А. Жертвы кибермошенничества как один из объектов современной кибервиктимологии: краткий статистический анализ показателей криминальной виктимности 2021 - 2022 гг. / П. А. Кабанов // Виктимология. - 2023. - Т. 10. - № 1. - С. 17-28.
22. Квасникова Т. В. Новые направления мошеннических посягательств с использованием цифровых технологий / Т. В. Квасникова // Таможенная политика России на Дальнем Востоке. - 2024. - № 2(107). - С. 81-86.
23. Мартьянов Н. Р. Уголовно - правовая борьба с киберпреступлениями на современном этапе / Н. Р. Мартьянов // Государственная служба и кадры. - 2020. - № 1. - С. 175- 177.
24. Маилян А. В. Актуальные вопросы расследования и раскрытия кибермошенничества «фишинг» /А. В. Маилян // Философия права. - 2022. - № 2 (101). - С. 112 - 115.
25. Майор А. А. Система мер противодействия мошенничеству и его распространению в российской федерации /А. А. Майор // Вестник науки. - Т.2. - 2020. - № 7 (28). - С. 73- 75.

26. Наймушина К. М. Современное состояние киберпреступности: мошеннические схемы в сети интернет / К. М. Наймушина, А. П. Беляев // Вестник науки. - 2024. - №5 (74). - том 3. - С. 477 - 483.
27. Намысов Е. Д. Мошенничество в цифровую эпоху в связи с общественными изменениями / Е. Д. Намысов // Криминологический журнал. - 2023. - № 3. - С. 148 - 154.
28. Родивилина В. А. Мошенничество в информационно-телекоммуникационных сетях / В. А. Родивилина, В. В. Коломинов // Криминалистика: вчера, сегодня, завтра. - 2022. - № 4 (24). - С. 143- 151.
29. Ройхка А. А. Зарождение киберпреступности и этапы её последующего генезиса: российский и зарубежный опыт / А. А. Ройхка // Молодой ученый. - 2025. - № 13 (564). - С. 130-131.
30. Струков А. Е. Понятие и способы мошенничества / А. Е. Струков // Вестни магистратуры. - 2022. - № 1- 2 (124). - С. 10- 12.
31. Сульгина В. С. Кибермошенничество: виды, схемы, способы противодействия / В. С. Сульгина, Е. В. Мацкайлова // Материалы XXV Международного конкурса научно-исследовательских и творческих работ учащихся «Старт в науке». - М., 2023. - С. 4 - 22.
32. Тимофеев А. В. Киберпреступность как социальная угроза и объект правового регулирования / А. В.Тимофеев, А. А. Комолов // Современные философские исследования. - 2021. - № 1. - С. 96- 99.
33. Шалагин А. Е. Трансформация преступности в XXI веке: особенности предупреждения и противодействия / А. Е. Шалагин, А. Д. Идиятуллов // Вестник Казанского юридического института МВД России. - 2021. - Т. 12. - № 2(44). - С. 227- 235.
34. Ширшиков А. С. Мошенничество как вид цифровой преступности / А. С. Ширшиков // Молодой ученый. - 2022. - № 51 (446). - С. 591- 594.
35. Шишкина М. В. Мошенничество с использованием информационных технологий: современные вызовы и ответы / М. В.

Шишкина, Э. Ю. Латыпова // Научный лидер. - 2025. - №17 (218). - С. 240 - 241.

Источники на электронных носителях

36. Жители Пензенской области за год перечислили мошенникам более 1 млрд рублей. - URL: <https://penzavzglyad.ru/news/176923/zhiteli-penzenskoy-oblasti-za-god-perechislili-moshennikam-bolee-1-mlr-rubley> (дата обращения: 05.04.2025).

37. Как не стать жертвой киберпреступлений. - URL: https://penza.sledcom.ru/Poleznaja_informacija/item/1165598/ (дата обращения: 03.04.2025).

38. Кампания по повышению уровня финансовой киберграмотности населения. - URL: <https://disk.yandex.ru/d/ju-52sM455e19g> (дата обращения: 03.04.2025).

39. Кибермошенничество: портрет пострадавшего. - URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения: 29.03.2025).

40. Органы прокуратуры области принимают меры по защите прав потерпевших по уголовным делам о телефонных мошенничествах. - URL: https://epp.genproc.gov.ru/web/proc_58/mass-media/news?item=100258785 (дата обращения: 05.04.2025).

41. The 24/7 Network established under the Convention on Cybercrime (known as the Budapest Convention) / Council of Europe 2016. - URL: <https://www.coe.int/en/web/cybercrime/24/7-network-new> (дата обращения: 05.04.2025).



Рис.4 Кампания по повышению уровня финансовой киберграмотности населения¹

¹ Кампания по повышению уровня финансовой киберграмотности населения. - URL: <https://disk.yandex.ru/d/ju-52sM455e19g> (дата обращения: 03.04.2025).