**УДК 34**

# Виды и способы совершения мошеннических преступлений в сети Интернет

**Нуруллина Гульфиза Мазитовна**

Кандидат политических наук,
доцент кафедры юридических и гуманитарных дисциплин,
Набережночелнинский филиал ТИСБИ,
423800, Российская Федерация, Набережные Челны,
ул. Комсомольская Набережная, 6;
e-mail: nurullina@inbox.ru

**Мугинова Назира Халитовна**

Кандидат социологических наук,
доцент кафедры юридических и гуманитарных дисциплин,
Набережночелнинский филиал ТИСБИ,
423800, Российская Федерация, Набережные Челны,
ул. Комсомольская Набережная, 6;
e-mail: nurullina@inbox.ru

**Харисова Эльвира Анваровна**

Старший преподаватель
кафедры юридических и гуманитарных дисциплин,
Набережночелнинский филиал ТИСБИ,
423800, Российская Федерация, Набережные Челны,
ул. Комсомольская Набережная, 6;
e-mail: nurullina@inbox.ru

**Аннотация**

Интернет – огромная сеть безграничных возможностей, где каждый день проходят: сделки, покупки, лотереи, конкурсы, а также очень часто происходят махинации, в которые можете попасть и вы. Актуальность данной темы и вызвана тем, что мошенничество становится наиболее распространенным компонентом телефонных и интернет-преступлений, о котором необходимо предупреждать и обезопасить себя и близких, и не стать жертвой интернет-аферы. Мошенников можно разделить на следующие категории в зависимости от их способа действия, размера понесенных потерь и характеристик преступника по статьям 159 либо 159.6 Уголовного кодекса Российской Федерации. Для защиты от этого есть способы контроля и надзора. Ежедневно отделения по борьбе с кибер-преступниками находят различные приемы, способы, методы, которыми пользуются мошенники, как например: фальшивые сайты с безумным выигрышем, сайты с привлекательной рекламой и т.д. Борьба с этим происходит каждый день и развитие

проблемы, и решение ее прогрессирует с невероятной скоростью. Можно сделать определенные выводы о способах таких преступлений. Что, в свою очередь, позволит разработать действия по борьбе с интернет-мошенниками и обезопасить граждан. Несмотря на имеющийся у нас опыт расследования и рассмотрения уголовных дел указанной категории, мы должны тщательно помнить о необходимости проверки информации при совершении телефонных звонков с незнакомыми людьми и совершении финансовых операций в сети Интернет.

**Для цитирования в научных исследованиях**

Нуруллина Г.М., Мугинова Н.Х., Харисова Э.А. Виды и способы совершения мошеннических преступлений в сети Интернет // Вопросы российского и международного права. 2024. Том 14. № 4А. С. 552-563.

**Ключевые слова**

Интернет, фишинг, кардинг, преступник, противоправные действия, мошенничество в интернете, методы, схемы, данные, финансы.

## Введение

В интернете существуют разные виды схем и возможностей, например, для оформления документов, осуществление финансовых операций, управление накопительными счетами с помощью онлайн сервисов, но благодаря такому развитию, в хорошем ключе, зародилась и плохая сторона этой истории, такая, как небывалая активность аферистов в интернете. Зная, что в интернете не нужно общаться в живую, что затрудняло бы мошенническую деятельность, поэтому с помощью социальных сетей, форумов доверчивых граждан стало легче обмануть. Частыми способами являются:

Фишинг – это кража личных данных (например, имен, паролей, данных банковских карт). Преступники пользуются беспечностью людей и получают конфиденциальную информацию путем создания поддельных веб-сайтов, липовых аккаунтов, аккаунт-ботов в социальных сетях и отправки электронных писем, как и на почту, так и в сообщениях, к примеру, предложение перейти на сайт, где человеку якобы присужден подарок. Преступники выдают себя за заслуживающие доверия источники в Интернете и заставляют жертв предоставлять личную информацию.

Кардинг – это вид интернет-преступления, где преступник или группа лиц, путем обмана или вредоносных ПО (программное обеспечение), выманивают данные банковских карт или снимают с них денежные средства, воруют личную информацию людей. Больше всего такое происходит с серверами интернет-магазинов.

Ежедневно появляется много фальшивых сайтов, площадок. Чаще всего используют медицинские маски, перчатки, антисептические средства, вакцины и препараты, обработка квартир, химчистка. Обманутые пользователи, переходя на сайт с фальшивым оформлением, затем проходят по заполнению заявки на заказ и вводят данные карты в якобы предназначенные места для карт оплаты. И после оплаты теряют свои денежные средства и также передают тем самым информацию о банковской карте [Гармышев, 2021].

Цель нашего исследования – выявление способов совершения мошеннических телефонных и интернет-преступлений, о которых необходимо предупреждать, чтобы обезопасить себя и близких, и не стать жертвой интернет-аферы.

## Основная часть

Документальной основой для изучения и анализа данной темы стал Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.12.2022, с изм. от 15.03.2023), п.1 ст.273, а также авторские материалы Я.В. Гармышева, Д.С. Рожковой, Д.А. Муромской, М.М.Милованова, В.А. Шурухнова и др.

Мошенники преследуют только одну цель: обмануть людей и завладеть деньгами или имуществом. Они знают, как очаровать, как использовать чувства и эмоции и как запугать. Среди них есть психологи, эксперты в области экономики, финансов и страхования.

Самые распространенные схемы мошеннических действий в киберпространстве:

*Двойники интернет-магазинов*. Обычно представляют собой какую-нибудь пародию на популярный сайт продаж товаров, и как бы невзначай выставляет огромные скидки, доверчивые люди, переходя на сайт, регистрируются и заполняют форму для покупки товара, где вводят данные карты, и после оплаты продавец пропадает и деньги тоже. Важно знать, что самым простым способом обезопасить себя является проверка адресной строки в браузере. Но это не гарантирует полностью безопасность данных, хотя можно будет отличить сайт-подделку от настоящего, тем, что большинство безопасных сайтов начинается с https – (безопасный протокол передачи данных).

Похожими двойниками можно назвать копии сайтов или каких либо сервисов интернет-банкинга, где мошенники отправляют на мобильный телефон СМС или электронное письмо на почту под предлогом пройти на их сайт для просмотра новых акций, проверки статуса заявки, или с тем, что появилось выгодное предложение. После чего невнимательные граждане проходят и заполняют данные для входа в личный кабинет от их финансов. Ну, а после этого злоумышленники, просто пользуясь данными, снимают все средства.

*Фишинговая атака по электронной почте*. Отправка писем с текстом о победе в розыгрыше и т.д. И всегда просят оплатить сумму перевода или заплатить определенную сумму, неполную, для активации карты.

Взламывают аккаунты и отправляют поддельные сообщения друзьям, чтобы получить деньги. Преступники различными ситуациями обманывают друзей или родственников для получения денег и в последнее время довольно креативно это делают.

*Обманные сайты с благотворительностью, туроператоров или авиакомпании*. Требуют якобы оплатить лечение человеку с сильной болезнью, или огромные скидки на путевки.

*Различные предложения с отличным заработком.* По типу удаленной работы, но почти сразу просят оплатить организационные нужды. После перевода средств работодатель пропадает.

Личная конфиденциальная информация – эти данные легко заполучить с помощью вирусов и сбора пользовательской информации [Рожкова, Муромская, 2022].

Самым легким видом преступлений считаются потенциально нежелательные программы (ПНП или PUP). Все потому, что они могут скачивать вредоносные программы, перенаправлять вас на ненадежные сайты, с целью скачивания вирусов и другого нежелательного контента, также может удалять установленное ПО или включать шпионское либо рекламное. А легким оно является, потому что решение данной проблемы очень простое – нужно скачать антивирус.

Также известно, что при разбирательстве с вредоносными программами, если пострадавший утратил какие-либо данные со своих устройств из-за вредоносного ПО, то создатель этого ПО

будет нести срок до 4-х лет тюрьмы, или иным представленным судом наказанием предусмотренной статьей 273 УК РФ.

Многие СМИ и полиция рассказывали об интернет-аферах и предупреждали, об их возможности, а также рассказывали, как с ними бороться. Но не только методы борьбы изменились, но и сами мошенники эволюционируют.

Даже недавно мошенники снова нашли новые методы обмана людей с помощью транзакций за онлайн-услуги и выгодные предложения в качестве помощи.

Для помощи, если вас обманули, или были совершены мошеннические действия, нужно:

– обратиться в службу поддержки банка или в компанию, занимающуюся денежными переводами, чтобы заблокировать счет;
– для получения помощи полиции можно сделать звонок или посетить сайт Министерства внутренних дел Российской Федерации. Для этого создали отдел, специализированный под преступления в сфере компьютерной безопасности Управление «К»;
– в Роскомнадзор, так как он производит надзор за компаниями, специализирующимися в сфере электронных технологий. Если у мошенников имеется вредоносный сайт, его можно быстро заблокировать, сообщив об этом в Яндекс или Google. Если же данное обоснование будет подтверждено убедительными фактами, пострадавшему нужно указать в заявлении:
– данные из паспорта, такие как ФИО, адрес регистрации и его контактный номер телефона;
– четко описать ситуацию с указанным датой, временем и местом совершения мошенничества, а также обстоятельства, которые сопутствовали к его обману;
– дата подачи заявления и подпись.

Немаловажный пункт – нужно будет приложить документы, подтверждающие факт мошенничества.

Уголовная ответственность по статье 159.6 УК РФ наступает с момента получения потерпевшим заявления о причинении вреда в размере 2500 рублей.

Наказания за этот инцидент, следующие:

– административный штраф до 120 т.р.
– обязательные работы до 360 часов;
– исправительные работы до одного года;
– ограничение свободы или взамен этому принудительные работы до 2-х лет;
– возможный арест до 4-х месяцев;
– возможное лишение свободы до 2-х лет.

Стоит отметить, что, если преступление было совершено группой лиц по предварительному сговору, наказание будет в виде лишения свободы до 10 лет.

Может возникнуть вопрос, можно ли и как вернуть свои сбережения, после того как против вас были совершены противозаконные действия мошенничества, если вы обратитесь в полицию сразу, то это позволит быстро начать оперативные мероприятия для восстановления справедливости.

Но есть небольшой нюанс, если гражданин в течение суток обратился в полицию, то в соответствии со статьей 29 ФЗ «О национальной платежной системе» банк обязан возвратить средства. Финансово-кредитное учреждения в течение 30 дней проводит расследование и после принимает решение о погашении или отказе в выдаче денежных средств. Но если получилось

так, что пострадавший собственноручно передал 3-им лицам PIN-код, то его средства вернуть не удастся.

Чтобы обезопасить себя и близких, и не стать жертвой, нужно быть внимательным при совершении любых онлайн транзакциях, покупках по банковской карте и т.д. Важно не раскрывать никому данные ваших банковских карт. Ведь вы могли заметить, что настоящие работники банков не спрашивают и не требуют у вас данные с этой карты, есть исключения в виде последних цифр номера самой карты, но никак не код (CVC) от нее.

Существуют правила, как обезопасить себя в сети «интернет»:

– иметь хотя бы одну виртуальную карту для покупок и пополнять ее только в случае покупки;
– необходимо создавать довольно сложные пароли и пользоваться разными данными для электронной почты, социальных сетей и т.д. Ведь легче восстановить пароль, а не мучится с возвратом денежных средств;
– определенно важным аспектом будет то, что вы не должны переходить на подозрительные сайты, не нажимать на подозрительные ссылки и т.д., если вам поступили такие сообщения, то удалите их или проигнорируйте;
– не передавать или не сообщать ваши личные или банковские данные третьим лицам и не вводить их в небезопасные, непроверенные сайты. А также не сообщайте коды из сообщений;
– очень внимательно проанализируйте сообщение или информацию, предоставленную вам от друзей, родственников или знакомых в социальных сетях, лучше позвоните им и уточните все ли у них в порядке. В противном случае может оказаться, что сообщение, полученное от них в социальных сетях, было обманом мошенников о просьбе денежных средств;
– использовать в незнакомых местах VPN (Virtual Private Network) анонимный (приватный) доступ в Интернет, чтобы мошенники не могли скачать с устройства личные данные.

Как обезопасить себя и не стать жертвой мошенников?

Чтобы не быть обманутыми мошенниками, будьте осторожны при совершении денежных операций с банковской картой и никогда не передавайте информацию о своей карте третьим лицам. Любые работники банков никогда не запрашивают у клиентов номер CVV/CVC на обороте карты.

Обезопасить свои финансы позволит соблюдение базовых правил:

– Можно пользоваться созданной вами в личных кабинетах банков виртуальной картой для покупок. Рекомендуется пополнять только один раз перед оплатой.
– Меняйте пароль хотя бы каждые 2-3 месяца, но важно, чтобы эти пароли были сложные, так как восстановить пароль можно быстро и удобно, а вернуть деньги получится не всегда.
– Не переходите по незнакомым ссылкам, предоставленным электронными письмами, мессенджерами или социальными сетями, особенно ссылкам, рекламирующими что-то бесплатно или на выгодных условиях.
– Не сообщайте другим данные карты, не заходите на незнакомые сайты и не указывайте коды безопасности в текстовых сообщениях.
– Критически оценивать всю информацию, новости, рекламу в интернете, а также не верить

на слово внезапным обращениям от друзей и родственников, возможно, вы получили СМС от мошенника, который взломал их аккаунт.

– Использовать в незнакомых местах VPN (Virtual Private Network) анонимный (приватный) доступ в Интернет, чтобы мошенники не могли скачать с устройства личные данные.

Также хотелось добавить, чтобы обезопасить себя, рассматривая все виды преступлений в сети Интернет, необходимо соблюдать определенные правила работы в сети, самые важные стоит подчеркнуть:

– Регулярное обновление софта и ОС.

– Соблюдение этих рекомендаций поможет защитить ваш компьютер с помощью исправлений безопасности.

– Установите антивирусную программу с регулярными обновлениями.

– Используйте антивирусную программу или встроенное комплексное решение для вашей сети. Работа антивирусного программного обеспечения заключается в отслеживании, обнаружении и удалении угроз до того, как они вызовут проблемы. Это программное обеспечение защищает ваш компьютер и личную информацию от киберпреступников и атак вредоносного ПО. Для обеспечения максимальной защиты антивирусную программу необходимо регулярно обновлять.

– Используйте надежные пароли.

– Устанавливайте сложные пароли, которые трудно угадать, храните их только в голове и у единственного ответственного сотрудника, подписавшего приложение об индивидуальной ответственности. Вы можете использовать администратора для создания надежных паролей.

– Остерегайтесь спама.

– Не открывайте вложения и не переходите по ссылкам в подозрительных электронных письмах. Рассылка спам-сообщений с вложениями – наиболее распространенный способ заражения ПК вирусами и совершения других видов киберпреступлений. Если отправитель неизвестен, письмо лучше проигнорировать.

*Защита коммерческой информации.*

Вы не должны разрешать доступ к своим личным данным по телефону или электронной почте, не убедившись в безопасности вашего телефонного соединения и электронной почты.

*Личный звонок при получении подозрительного запроса.*

Личная и деловая информация, которую запрашивает сотрудник компании, но личность звонившего неизвестна. Лучше просто повесить трубку и проверить номер вызывающего абонента. Потом можно перезвонить на официальный номер компании и организации и убедиться, что звонок не от мошенника. Мы рекомендуем использовать для звонка другой телефон, так как злоумышленник может повесить трубку.

*Проверка веб-адресов при посещении ресурсов в сети.*

Все пользователи локальной сети должны обращать внимание на URL-адреса сайтов для посещения. Нельзя открывать ссылки, адреса которых выглядят незнакомо либо подозрительно. Если используемый антивирус включает защиту онлайн-транзакций, необходимо убедиться, что она активна, прежде чем давать сотрудникам право совершать какие-либо действия.

*Будьте осторожны при просмотре банковской информации.*

Важно определить точный момент, когда организация становится жертвой мошенников.

Необходимо внимательно изучить свои банковские выписки и запросить неизвестные и сомнительные детали транзакции. Банки могут проверить их на мошенничество.

Наименее заметным является мошенничество на сайтах знакомств. На таких сайтах в процессе общения должны быть заинтересованы обе стороны, но иногда все не так. Мошенники маскируются под женщин (или мужчин), не публикуя свои фотографии, а заманивают осторожных пользователей со стоковых сервисов (стоковые сервисы – это веб-сайты, которые предлагают фотографии определенного предмета для продажи в качестве рекламы или иллюстрации) завлекая пользователей связаться с ними. Во время разговора может быть непонятно, что это мошенничество, но, когда дело доходит до действия, например, пойти на свидание или встречу, мошенники могут потребовать от пользователей определенную сумму денег. Билеты, еда, больничные для (его) близких или просто в качестве подарка. В таких случаях желательно заранее проверить, настоящий ли профиль. В борьбе с этим веб-сайты часто используют какой-либо индикатор, указывающий на проверенную учетную запись пользователя. Кроме того, боты (искусственный интеллект, запрограммированный для простых функций, таких как списки рассылки), могут бесконечно связываться со всеми пользователями службы и отправлять или обманом заставлять их загружать вредоносные программы и т.д. Сайты и сервисы часто предлагают новые способы борьбы с этим, которые в большинстве своем помогают в краткосрочной перспективе, а также способы помочь владельцам интернет-ресурсов, отправляя жалобы на их аккаунты этих ботов или мошенников, которых пропустила система контроля.

Если рассматривать нововведения со стороны безопасности, то, к сожалению, чем больше технологий, чем больше разных защитных или нет сервисов, тем больше и быстрее увеличивается и число преступлений.

Мошенничество, связанное с хищением имущества или приобретением имущественных прав путем проникновения, удаления, блокирования, изменения или вмешательства в хранение, обработку или передачу компьютерных данных или информационно-коммуникационных сетей, зависит, прежде всего, от обстоятельств, при которых произошло преступление [Шиганов, Чеджемов, 2019].

Мошенничество является наиболее распространенным компонентом телефонных и интернет-преступлений. Мошенники очень умны по части психологии, с помощью этого они ловко получают информацию путем общения, даже если жертва думает, что говорит простые вещи, они могут стать ключевыми или важными для мошенника. Каждый может быть жертвой любого вида мошенничества. Мошенники часто пользуются предлогами о плохом или плачевном состоянии родных жертв, или безопасностью счетов в банках и т.д. Основными видами «телефонного» мошенничеств являются:

– звонки от имени полиции о том, что родственник попал в ДТП, в полицию, в больницу и т.п., в связи с чем, для освобождения от уголовной ответственности, требуют передать определенную сумму денег;
– звонки о желании приобрести какое-либо имущество, размещенное на различных Интернет-сайтах гражданами в объявлениях о продаже: в этом случае мошенник находит номер в объявлении, звонит и просит продиктовать номера банковских карт, для перевода денег за товар, далее просит код доступа, для ареста банковского счета жертвы;
– звонок одного из сотрудников банка, касательно вопросов о взломе его мобильного приложения, постороннего входа, задолженности перед банком или кредитной

организации и многом другом.

Некоторые эксперты также могут порекомендовать быть более осторожными с приложениями, которые вы используете и загружаете. Например, где вы скачиваете музыку и видео? Оно может содержать вредоносное ПО или быть инструментом взлома. Чтобы обезопасить пользователей некоторые из них ввели функцию «подтверждение входа». Например, для входа с другого устройства или браузера и для этого как раз и ввели подтверждения с помощью кода из СМС [Стеценко, Холодковская, 2021].

Во время общения мошенник запросит другой код доступа или использует транзакцию, позволяющую получить доступ к банковскому счету жертвы.

СМС или звонок о выигрыше ценного приза, ради которого нужно перевести предоплату. Самые распространенные, часто используемые виды мошенничества в Интернете: это те сайты бесплатных объявлений бесплатных объявлений («Avito», «AutoRU» и т.д.), где мошенники предлагают купить или продать недвижимость с последующей предоплатой или предоплатой мошенника во время общения. Благодаря вирусам, со сторонних программ, сайтов или спам-рассылки мошенники, могут получить доступ ко всему, что им нужно. Часто люди могут столкнуться с рекламой о больном ребенке и т.д., что в свою очередь переход на такую вида рекламу повлечет за собой не моментальный, но скорейший процесс, либо заражения компьютера, кража информации из браузера и т.д. Такая реклама может быть полностью вымышленной или использовать настоящую рекламу, например, рекламные ролики.

Однако для начала работы, как правило, требуется оплата за приобретение так называемого «стартового набора» или подписка на платные интернет-ресурсы. В результате рабочие материалы так и не поступают или же в ответ им присылают ненужную информацию с бесплатного источника, также рекламное привлечение в финансовую пирамиду и т.д.

Приведенные выше схемы телефонного и онлайн-мошенничества не являются исчерпывающими, существует множество их вариаций и новых механизмов, регулярно разрабатываемых мошенниками для хищения денег. Однако во всех случаях цель состоит в том, чтобы убедить людей передать деньги «добровольно». Мошенников можно разделить на следующие категории в зависимости от их способа действия, размера понесенных потерь и характеристик преступника по статьям 159 (Мошенничество) либо 159.6 (Мошенничество в сфере компьютерной информации) Уголовного кодекса Российской Федерации. Несмотря на имеющийся у нас опыт расследования и рассмотрения уголовных дел указанной категории, мы должны тщательно помнить о необходимости проверки информации при совершении телефонных звонков с незнакомыми людьми и совершении финансовых операций в сети Интернет.

Серьезно важна проблема быстрого распространения идей террористического и экстремистского направления, распространения материалов, возбуждающих межнациональную и межрелигиозную рознь [Шеметов, Комоско, Васюков, 2021], рассылки постов, призывающих к суициду [Кот, 2020], совершения преступлений против половой неприкосновенности несовершеннолетних с использование современных информационных технологий и т.д. [Живодрова, Толоконникова, 2020].

Мы также наблюдаем развитие цифровизации, совершенствование интернет-технологий и увеличение видов мошенничества, таких как интернет-банкинг. Но со временем и это, с более быстрым интернетом и беспроводной передачей данных (WIFI) и отказом от наличного денежного обращения и использованием безналичных расчетов, эта проблема решалась быстрее [Фатахова, 2020].

Верховный суд в 2022 году установил, что выявить место преступления не всегда легко. Таким образом, было решено: оно определяется как место совершения правонарушения, входящее в состав объективной стороны преступления. Учитывая экстремистскую деятельность, место становится территорией, где преступники используют устройства. Однако, когда преступление совершается дистанционно, а преступник находится в другом месте, или когда атака осуществляется автоматически с помощью алгоритма, возникает много вопросов, поскольку место происшествия не всегда четко. Поэтому мы предполагаем, что это место, где будет закончено досудебное расследование.

Бывают случаи, когда проблемы, вызванные вирусами, не считаются преступными. Эти случаи редки. То есть: ваш вирус был создан вами и распространен на ваше устройство только в целях безопасности или в образовательных целях. Другими словами, у пользователей не было корыстных мотивов уничтожать, блокировать, передавать или незаконно получать доступ к данным в обход мер безопасности.

Также не стоит забывать, что по незнанию или неосторожности, ни в коем случае нельзя выставлять, выкладывать, указывать свои данные личного характера, все мы должны понимать, что любую информацию можно обратить против себя, как например: выставление паролей в виде своих любимых дат, и пометкой их в социальных сетях, но если вам нравится чтобы был такой пароль, добавьте к нему, слова, символы, чтобы его не так легко было взломать, также с кличками ваших домашних питомцев и т.д. Мы рекомендуем использовать надежные пароли и случайные комбинации. Если вы думаете, что вдруг забудете свой пароль, запишите его только там, где вы можете получить к нему доступ, а не на своем компьютере или мобильном устройстве. Но даже если есть сомнения, безопаснее всего создавать пароль каждый месяц или реже по своему усмотрению.

Официальные статистические данные, подтверждающие вышеизложенное, свидетельствуют о резком росте компьютерной преступности в последние годы. Так, во втором полугодии 2021 года правоохранителями зарегистрировано 375 892 таких правонарушения, из них 24 561 с использованием компьютерных устройств и 178 944 с использованием средств мобильной связи. Программные инструменты – 9 623, Интернет-сети – 183 765. По статье 159.6 было инициировано 849 незаконных действий. Приведенные данные свидетельствуют о том, что общее количество преступлений с использованием информационно-коммуникационных технологий увеличилось на 40% по сравнению с аналогичным периодом прошлого года. Основная причина беспрецедентного роста интернет-мошенничества является доступность компьютерного оборудования и информационно-коммуникационных технологий [Милованова, Шурухнов, 2021].

С применением методов анализа, изучив тему мошеннических преступлений в сети Интернета, можно сделать определенные выводы о способах таких преступлений. Что, в свою очередь, позволит разработать действия по борьбе с интернет-мошенниками и обезопасить граждан.

На данный момент обществу стало удобнее распознавать разные ситуации в Интернете. По типу: мошенничество, преследование или другие преступления, связанные с использованием ценных информационных средств. Ибо справедливость в этот момент можно обрести, и добиться ее нетрудно. Поскольку компании и сайты в социальных сетях ввели усиленную защиту в виде двухэтапной идентификации или начали некоторое время хранить информацию о ваших действиях на своих серверах, в случае незаконной активности, совершая нарушения, их

можно отследить. А с юридической стороны правоохранительные органы уже разработали немало схем и комбинаций для ловли преступников в Интернете.

Для защиты от этого есть способы контроля, надзора. Ежедневно отделения по борьбе с кибер-преступниками находят различные приемы, способы, методы которыми пользуются мошенники, как например: фальшивые сайты с безумным выигрышем, сайты с привлекательной рекламой и т.д. Борьба с этим происходит каждый день и развитие проблемы, и решение ее прогрессирует с невероятной скоростью.

## Заключение

Несмотря на имеющийся у нас опыт расследования и рассмотрения уголовных дел указанной категории, мы должны тщательно помнить о необходимости проверки информации при совершении телефонных звонков с незнакомыми людьми и совершении финансовых операций в сети Интернет.

## Библиография

1. Гармышев Я.В. Квалификация мошенничества с использованием компьютерных технологий. Вопросы законодательства и правоприменительной практики // Закон и право. 2021. № 2. С. 76.
2. Живодрова Н.А., Толоконникова А.С. Интернет-пространство как средство совершения преступлений против половой неприкосновенности несовершеннолетних // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования. Иркутск, 2020. С. 64.
3. Кот Е.А. Особенности преступлений, совершенных в сети Интернет, связанных с побуждением несовершеннолетних к самоубийству // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 4. С. 94.
4. Милованова М.М., Шурухнов В.А. О способах мошенничества в сети «интернет» // Имущественные отношения в Российской Федерации. 2021. № 10 (241). С. 86.
5. Рожкова Д.С., Муромская Д.А. Мошенничество в интернете// Вестник ПензГУ. 2022. № 3 (39). С. 94-98.
6. Стеценко Ю.А., Холодковская Н.С. Мошенничество в сети интернет // Вестник Таганрогского института имени А.П. Чехова. 2021. № 2. С. 74.
7. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.12.2022, с изм. от 15.03.2023).
8. Фатахова Д.Р. Мошенничество в сети интернет // Молодой ученый. 2020. № 49 (339). С. 341.
9. Шеметов А.К., Комоско А.А., Васюков В.Ф. Отдельные аспекты противодействия преступлениям экстремистской и террористической направленности, которые совершаются с использованием сети Интернет // Современное общество и право. 2021. № 6. С. 6.
10. Шиганов В.А., Чеджемов Г.А. Мошенничество в сети интернет и способы защиты от него // Интернаука. 2019. № 16 (98). С. 33.

## Types and methods of committing fraudulent crime on the Internet

**Gul'fiza M. Nurullina**

PhD in Political Science,
Associate Professor of the Department of Legal and Humanitarian Disciplines,
University of Management – TISBI,
Branch in Naberezhnye Chelny,
423800, 6, Komsomol'skaya Naberezhnaya str.,
Naberezhnye Chelny, Russian Federation;
e-mail: nurullina@inbox.ru

**Nazira Kh. Muginova**

PhD in Social Sciences,
Associate Professor of the Department of Legal and Humanitarian Disciplines,
University of Management – TISBI,
Branch in Naberezhnye Chelny,
423800, 6, Komsomol'skaya Naberezhnaya str.,
Naberezhnye Chelny, Russian Federation;
e-mail: nurullina@inbox.ru

**El'vira A. Kharisova**

Senior Lecturer at the Department of Legal and Humanitarian Disciplines,
University of Management – TISBI,
Branch in Naberezhnye Chelny,
423800, 6, Komsomol'skaya Naberezhnaya str.,
Naberezhnye Chelny, Russian Federation;
e-mail: nurullina@inbox.ru

**Abstract**

The Internet is a huge network of endless possibilities, where every day there are deals, purchases, lotteries, contests, and very often there are frauds that you can get into. The relevance of this topic is due to the fact that fraud is becoming the most common component of telephone and Internet crimes, about which it is necessary to warn and protect yourself and loved ones, and not become a victim of an Internet scam. Fraudsters can be divided into the following categories depending on their mode of action, the amount of losses incurred and the characteristics of the offender under Articles 159 or 159.6 of the Criminal Code of the Russian Federation. To protect against this, there are ways of control, supervision. On a daily basis, cybercrime departments find various tricks, methods used by scammers, such as: fake sites with insane winnings, sites with attractive advertising, etc. The struggle with this is happening every day and the development of the problem, and its solution is progressing at an incredible speed. With the use of analysis methods, having studied the topic of fraudulent crimes on the Internet, it is possible to draw certain conclusions about the methods of such crimes. Which, in turn, will allow developing actions to combat online fraudsters and protect citizens. Despite our experience in investigating and considering criminal cases of this category, we must carefully remember the need to verify information when making phone calls with strangers and making financial transactions on the Internet.

**For citation**

Nurullina G.M., Muginova N.Kh., Kharisova E.A. (2024) Vidy i sposoby sovershenia moshennicheskikh prestuplenii v seti Internet [Types and methods of committing fraudulent crime on the Internet]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 14 (4A), pp. 552-563.

**Keywords**

Internet, fishing, carding, criminal, fraud, illegal actions, fraud on the Internet, methods, schemes, data, finance.

## References


1. Fatakhova D.R. (2020) Moshennichestvo v seti internet [Fraud on the Internet]. *Molodoi uchenyi* [Young scientist], 49 (339), p. 341.
2. Garmyshev Ya.V. (2021) Kvalifikatsiya moshennichestva s ispol'zovaniem komp'yuternykh tekhnologii. Voprosy zakonodatel'stva i pravoprimenitel'noi praktiki [Qualification of fraud using computer technologies. Issues of legislation and law enforcement practice]. *Zakon i pravo* [Law and Right], 2, p. 76.
3. Kot E.A. (2020) Osobennosti prestuplenii, sovershennykh v seti Internet, svyazannykh s pobuzhdeniem nesovershennoletnikh k samoubiistvu [Features of crimes committed on the Internet related to inducing minors to commit suicide]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki* [News of Tula State University. Economic and legal science], 4, p. 94.
4. Milovanova M.M., Shurukhnov V.A. (2021) O sposobakh moshennichestva v seti «internet» [On methods of fraud on the Internet]. *Imushchestvennye otnosheniya v Rossiiskoi Federatsii* [Property relations in the Russian Federation], 10 (241), p. 86.
5. Rozhkova D.S., Muromskaya D.A. (2022) Moshennichestvo v internete [Fraud on the Internet]. *Vestnik PenzGU* [Bulletin of PenzSU], 3 (39), pp. 94-98.
6. Shemetov A.K., Komosko A.A., Vasyukov V.F. (2021) Otdel'nye aspekty protivodeistviya prestupleniyam ekstremistskoi i terroristicheskoi napravlennosti, kotorye sovershayutsya s ispol'zovaniem seti Internet [Certain aspects of countering extremist and terrorist crimes that are committed using the Internet]. *Sovremennoe obshchestvo i pravo* [Modern Society and Law], 6, p. 6.
7. Shiganov V.A., Chedzhemov G.A. (2019) Moshennichestvo v seti internet i sposoby zashchity ot nego [Fraud on the Internet and ways to protect against it]. *Internauka* [Interscience], 16 (98), p. 33.
8. Stetsenko Yu.A., Kholodkovskaya N.S. (2021) Moshennichestvo v seti internet [Fraud on the Internet]. *Vestnik Taganrogskogo instituta imeni A.P. Chekhova* [Bulletin of the Taganrog Institute named after A.P. Chekhov], 2, p. 74.
9. *Ugolovnyi kodeks Rossiiskoi Federatsii ot 13.06.1996 № 63-FZ (red. ot 29.12.2022, s izm. ot 15.03.2023*) [Criminal Code of the Russian Federation dated June 13, 1996 No. 63-FZ (as amended on December 29, 2022, as amended on March 15, 2023)].
10. Zhivodrova N.A., Tolokonnikova A.S. (2020) Internet-prostranstvo kak sredstvo sovershenіya prestuplenii protiv polovoi neprikosnovennosti nesovershennoletnikh [Internet space as a means of committing crimes against the sexual integrity of minors]. In: *Ugolovnyi zakon Rossiiskoi Federatsii: problemy pravoprimeneniya i perspektivy sovershenstvovaniya* [Criminal Law of the Russian Federation: problems of law enforcement and prospects for improvement]. Irkutsk.