Министерство просвещения Российской Федерации

Муниципальное бюджетное общеобразовательное учреждение

«Гимназия № 86 с углубленным изучением иностранных языков»

городского округа город Уфа Республики Башкортостан

**ПРОБЛЕМА ИНТЕРНЕТ-МОШЕННИЧЕСТВА В СОВРЕМЕННОЙ РОССИИ**

Автор проекта: Мышаков И.А.

ученик 9А класса

Руководитель: Носенко

Светлана Геннадьевна, учитель истории

МБОУ «Гимназия № 86»

Уфа - 2020

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc56190515)

[1 ИНТЕРНЕТ-МОШЕННИЧЕСТВО КАК НАИБОЛЕЕ АКТИВНО РАЗВИВАЮЩИЙСЯ ВИД ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ 5](#_Toc56190516)

[1.1 Понятие и виды мошенничества 5](#_Toc56190517)

[1.2 Статистика роста преступлений, совершаемых через интернет 7](#_Toc56190518)

[2 РАССЛЕДОВАНИЕ СЛУЧАЕВ ИНТЕРНЕТ-МОШЕННИЧЕСТВА ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ 14](#_Toc56190519)

[2.1 Выявление правоохранительными органами мошеннических действий в интернете 15](#_Toc56190520)

[2.2 Личность интернет-мошенника 18](#_Toc56190521)

[3 ПРЕДОТВРАЩЕНИЕ ИНТЕРНЕТ-МОШЕННИЧЕСТВА 21](#_Toc56190522)

[ЗАКЛЮЧЕНИЕ 25](#_Toc56190523)

[СПИСОК ЛИТЕРАТУРЫ 26](#_Toc56190524)

[Приложение А. Статистические данные 27](#_Toc56190525)

# **ВВЕДЕНИЕ**

Мошенничество одно из наиболее распространённых преступлений против имущества. Оно встречается в самых разных сферах жизнедеятельности и отличается большим количеством «сравнительно честных способов отъёма денег у населения». Количество преступлений, связанных с мошенничеством, постоянно растёт. Одновременно с развитием интернета увеличивается и количество мошенников, действующих через «всемирную паутину». Так, за время действия ограничений, связанных с эпидемией коронавируса, в России резко выросло число зарегистрированных случаев мошенничества. Об этом свидетельствует статистика Генпрокуратуры, проанализированная РБК [1]. При этом рост произошел исключительно за счет телефонного и интернет-мошенничества — за шесть месяцев 2020 года число случаев такого мошенничества выросло на 76% по сравнению с первым полугодием 2019 года. Мошенничество — одно из самых частых совершаемых в России преступлений, чаще регистрируются только кражи. Если последних за время самоизоляции стало меньше на 9%, то случаев мошенничества в совокупности — значительно больше, на 36% (ст. 159–159.6 УК РФ).

Практически все эксперты сходятся во мнении, что число киберпреступлений в будущем будет лишь возрастать, поскольку злоумышленники быстро адаптируют современные технологии, чтобы повысить свою эффективность. При этом доходы мошенников в мире исчисляются миллионами долларов. Из них только в США через интернет за 2019 год мошенники получили больше 70 млн долларов. И эти цифры будут расти.

Именно эти причины, а также доверчивость людей к влиянию мошенников вызвало мой интерес к данной теме и способам предотвращения этой проблемы.

Цель исследования – определить способы предотвращения интернет-мошенничества и возможные действия пользователей сети для избегания влияния мошенников.

Для достижения поставленной цели были сформулированы следующие задачи:

1. Рассмотреть феномен интернет-мошенничества, его виды
2. Проанализировать статистику роста случаев мошенничества в интернете за последние годы
3. Определить законодательную базу в области интернет-мошенничества и возможные действия правоохранительных органов.
4. Охарактеризовать психологический портрет мошенника и его вероятной жертвы.
5. Изучить наиболее действенные способы предотвращения интернет-мошенничества

Гипотеза исследования: мы предположили, что основным способом предотвращения интернет-мошенничества будет повышение уровня компьютерной грамотности и информационной безопасности населения.

Объект исследования – кибермошенничество.

Предмет исследования – способы предотвращения интернет-мошенничества.

Практическая значимость заключается в том, что данная работа будет способствовать повышению информационной безопасности и возможному снижению уровня интернет-мошенничества.

Проблема исследования. Нужно сказать, что одновременно с отмечаемым в последнее время ростом случаев мошенничества через интернет растет и количество работ, посвященных способам его предотвращения. В то же время данную тему нельзя назвать достаточно проработанной.

# **1 ИНТЕРНЕТ-МОШЕННИЧЕСТВО КАК НАИБОЛЕЕ АКТИВНО РАЗВИВАЮЩИЙСЯ ВИД ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ**

## **1.1 Понятие и виды мошенничества**

Под мошенничеством обычно понимается хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием. При этом под обманом понимается как сознательное искажение истины (активный обман), так и умолчание об истине (пассивный обман). В обоих случаях обманутая жертва сама передает своё имущество мошеннику.

Изначально слово «мошенничество» (по Соборному уложению Ивана IV Грозного) означало «обманное, ловкое (иногда внезапное) хищение чужого имущества». Первое законодательное определение мошенничества, близкое к современному, было дано в Указе Екатерины II от 3 апреля 1781 года «О разных видах воровства и какие за них наказания чинит»: «Будь кто на торгу… из кармана что вынет… или внезапно что отымет, или обманом или вымыслом продаст, или весом обвесит, или мерою обмерит, или что подобное обманом или вымыслом себе ему не принадлежащее, без воли и согласия того, чьё оно».

Мошенничество можно определить как «совершенные с корыстной целью путём обмана или злоупотребления доверием противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или иному владельцу этого имущества, либо совершенные теми же способами противоправное и безвозмездное приобретение права на чужое имущество».

Форма мошеннических обманов очень разнообразна. Обман может совершаться в виде устного или письменного сообщения, либо заключаться в совершении каких-либо действий: фальсификации предмета сделки, применение шулерских приёмов при игре в карты или «в напёрсток», подмена отсчитанной денежной суммы фальсифицированным предметом («куклой»), обвес и тому подобное. Очень часто обман действием сочетается со словесным.

Злоупотребление доверием может выступать в качестве самостоятельного способа мошенничества (например, при получении кредита, который должник не намерен возвращать), но чаще сочетается с обманом.

Большинство мошенников обладает глубокими знаниями в разных областях деятельности, в том числе в психологии, экономике, разных отраслях права, информационных технологиях. Нередко хорошо осведомлены о порядках и методах работы органов государственной власти и правоохранительных органов.

Мошенники широко используют приемы психологических манипуляций, в том числе часто следующие психологические уловки:

* предлагают совершить какую-либо сделку на условиях, которые значительно выгоднее обычных;
* заставляют жертву совершать какие-либо действия в спешке, мотивируя это различным образом;
* выдают себя за очень богатых, влиятельных и преуспевающих людей.

В соответствии с Уголовным кодексом РФ [2] можно выделить следующие виды мошенничества:

* мошенничество в сфере кредитования – хищение денежных средств заемщиком путем представления банку или иному кредитору заведомо ложных и (или) недостоверных сведений;
* мошенничество при получении выплат – хищение денежных средств или иного имущества при получении пособий, компенсаций, субсидий и иных социальных выплат, установленных законами и иными нормативными правовыми актами, путем представления заведомо ложных и (или) недостоверных сведений, а равно путем умолчания о фактах, влекущих прекращение указанных выплат;
* мошенничество с использованием электронных средств платежа;
* мошенничество в сфере страхования – хищение чужого имущества путем обмана относительно наступления страхового случая, а равно размера страхового возмещения, подлежащего выплате в соответствии с законом либо договором страхователю или иному лицу
* мошенничество в сфере компьютерной информации – хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

## **1.2 Статистика роста преступлений, совершаемых через интернет**

За время действия ограничений, связанных с эпидемией коронавируса, в России резко выросло число зарегистрированных случаев мошенничества. При этом рост произошел исключительно за счет телефонного и интернет-мошенничества — за шесть месяцев 2020 года число случаев такого мошенничества выросло на 76% по сравнению с первым полугодием 2019 года (рисунок А1). При этом тех же краж (самое большое количество преступлений в России связано именно с ними) за время самоизоляции стало меньше на 9%, а случаев мошенничества больше на 36% [3].

В целом массив преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, за последние 5 лет увеличился более чем в шесть раз с 43,8 тыс. преступлений в 2015 году до 294,4 тыс. в 2019 году (рисунок А2). По итогам первого полугодия 2020 г. их количество возросло почти на 92 % (до 225,5 тыс.). Если годом ранее такими деяниями было каждое девятое регистрируемое преступление, то сегодня это уже каждый пятый факт (рисунок А3) [4]. Больше половины от всех «киберпреступлений» (57 %) совершается с использованием сети «Интернет» (рисунок А4), свыше 40 % – при помощи средств мобильной связи. Более 80 % таких преступлений совершается путем кражи или мошенничества.

Всего с апреля по июнь прокуратура зафиксировала 82,5 тыс. случаев мошенничества, в том числе больше двух третей (71%) по телефону или через интернет. В аналогичный период прошлого года с помощью средств телекоммуникации совершалось только 50% мошенничеств, показывает статистика Генпрокуратуры. Это указывает на то, что общий прирост обеспечили именно эти способы обмана.

По сравнению с прошлым годом в Санкт-Петербурге число зарегистрированных случаев мошенничества выросло вдвое, в Москве — на 76%, в Свердловской области — на 60%, по Республике Башкортостан – на 45%.

По словам руководителя уголовной практики юридической фирмы “БиЭмЭс” Александра Иноядова, «в период карантина возникли новые поводы и основания для безналичных расчетов (рисунок А5). Росту числа мошенничеств также способствовало закрытие большинства торговых точек, собственники денежных средств более положительно, чем обычно, реагировали на предложения товаров и услуг на онлайн-площадках, чем воспользовались и мошенники. Например, возникли сайты-клоны известных торговых площадок по продаже дорогой компьютерной техники. Неопределенность с выплатами, требования самоизоляции при не всегда полном и доступном информировании позволяли мошенникам по надуманным основаниям вступать в контакт с пенсионерами, получать доступ к их банковским реквизитам, а иногда и неправомерно проникать в их жилище».

Компании в сфере компьютерной безопасности прогнозировали рост числа кибератак на незащищенные компьютеры и домашние сети сотрудников коммерческих компаний, в том числе финансовых, и эти, по мнению ряда экспертов, прогнозы сбылись.

В качестве примера часто встречающейся сейчас формы распространения вредоносных программ они приводят рассылки от имени авторитетных международных организаций, связанных со здравоохранением (ВОЗ, ЮНИСЕФ), которые получали сотрудники коммерческих компаний и госсектора России и стран СНГ. Так, только одной компанией, работающей в сфере компьютерной безопасности (Group-IB) за первый квартал этого года заблокировано около 5000 фишинговых ресурсов. Для сравнения: только за весь 2018 год было около 4400 ресурсов.

«В конце марта — начале апреля, когда столичные власти ограничили передвижения по городу, появились мошеннические сервисы: сайты, Telegram-каналы, VK и Instagram-аккаунты, предлагающие купить справки-пропуска на период карантина по цене от 3000 до 5500 руб. Всего мы обнаружили 185 мошеннических ресурсов, торгующих цифровыми пропусками», — добавил представитель Group-IB.

Площадкой для еще одной масштабной мошеннической схемы стали популярные сайты бесплатных объявлений. Злоумышленники размещали там лоты с намеренно заниженными ценами, а когда откликался потенциальный покупатель, присылали ему ссылку на фишинговую страницу якобы курьерского сервиса, прося перевести деньги за товар и доставку.

Массовый переход на удаленную работу и рост популярности онлайн-торговли привели к тому, что «число DDoS-атак за время карантина выросло на 15%, атак на сотрудников компаний, в первую очередь через фишинг, — на 10%; сами вредоносные рассылки стали более таргетированными и потому чаще вызывали доверие у получателей» [1].

Кроме фальшивых интернет-магазинов, «которые не занимались доставкой, а воровали платежные данные», наблюдался «существенный рост числа сайтов, предлагающих якобы простой и быстрый заработок, например, обещание заработка на майнинге криптовалюты. Это можно объяснить тем, что у ряда людей сократился личный доход во время глобальной пандемии и они стали более падки на предложения заработать много денег простым и быстрым путем» [1].

В апреле эксперты «Лаборатории Касперского» выявили 58 страниц, мимикрирующих под «Авито», а в июле — уже 201. Общее же число обнаруженных подделок под эту площадку за семь месяцев превысило 500. Также наблюдалось появление большого количества подозрительных ресурсов, якобы обещающих социальные выплаты в связи с пандемией или предлагающих пройти опрос за большое вознаграждение. Но получить деньги можно только после перевода «закрепительного платежа» или «комиссии». В результате деньги уходят злоумышленникам. Растет и активность злоумышленников, обзванивающих клиентов банков.

«Преступники умело встраиваются в новостную повестку. Так, совсем недавно они начали эксплуатировать тему вакцины от COVID-19: с 11 по 19 августа в наиболее популярных доменных зонах .com и .ru было зарегистрировано 107 доменов, содержащих в имени подстроку vaccin и имеющих отношение к коронавирусу и вакцине. Часть этих ресурсов впоследствии может использоваться злоумышленниками для фишинга» [3].

В начале 2020 года количество атак на россиян через скам-ресурсы (сайты, где под разными предлогами выманивают деньги), возросло в 10 раз до 15 млн, а число таких страниц увеличилось вдвое до 10 тыс. Об этом сказано в исследовании «Лаборатории Касперского» [4]. Резкий рост связан как с простотой и высокой «отдачей» этой схемы, так и с распространением коронавируса. Мошенники активно эксплуатируют тему пандемии: от фейковых обещаний выплачивать пособия или возмещения за небольшой денежный взнос до продажи индивидуальных средств защиты.

Если бы каждый переход на скамерскую страницу, который в итоге был заблокирован, повлек за собой обман хотя бы одного пользователя, то потенциальная сумма ущерба в первом квартале 2020 года могла превысить 3 млрд рублей, оценивается в исследовании. Эксперты не назвали, сколько денег россияне потеряли на скам-ресурсах за этот период [3].

Скам — это мошеннические рассылки и объявления, в которых пользователям обещают крупное денежное вознаграждение за прохождение опроса или участие в голосовании, поясняется в исследовании. При этом человеку нужно оплатить «комиссию» или «закрепительный платеж» на сумму порядка 200 рублей, которая попадает к злоумышленнику. Человек также рискует сохранностью своей платежной информации, если вводил данные карты.

Популярность скам-ресурсов связана с тем, что мошенникам не требуется специфических навыков для их создания, а изображения известных брендов повышают доверие потенциальных жертв. Резкий рост их числа в начале 2020-го может объясняться распространением коронавируса, поскольку россияне стали больше времени проводить дома, в интернете. Кроме того, на скам-ресурсах активно эксплуатируется тема пандемии: например, пользователям предлагают различные компенсации, для вывода которых нужно оплатить небольшую комиссию.

После выхода из режима самоизоляции могут стартовать массовые мошенничества с турпутевками на российские курорты, а также активизируются продавцы препаратов для восстановления сил, иммунитета и душевного здоровья. Новый импульс может получить и схема, когда людям предлагают привлекательную работу с условием предварительной оплаты обучения или методических материалов.

В последние годы широкую популярность получили смс-рассылки или электронные письма с сообщениями о выигрыше автомобиля либо других ценных призов. Для получения «выигрыша» злоумышленники обычно просят перевести на электронные счета определенную сумму денег, мотивируя это необходимостью уплаты налогов, таможенных пошлин, транспортных расходов и т.д. После получения денежных средств они перестают выходить на связь либо просят перевести дополнительные суммы на оформление выигрыша.

Еще один вариант – это «брачные мошенничества». Типичный механизм: с использованием сети Интернет преимущественно на сайтах знакомств преступники выбирают жертву, налаживают с ним электронную переписку от имени девушек, обещая приехать с целью создания в будущем семьи. Затем под различными предлогами «невесты» выманивают деньги (на лечение, покупку мобильного телефона, приобретение билетов, оплаты визы и т.д.). Переписка ведется главным образом студентами лингвистических ВУЗов. Направленные жертвами деньги преступники получают на подставных лиц. После получения средств переписка под различными предлогами прекращается.

Один из самых отвратительных способов хищения денежных средств – так называемый «крик о помощи». В интернете появляется душераздирающая история о борьбе маленького человека за жизнь. Время идёт на часы. Срочно необходимы дорогие лекарства, операция за границей и т.д. Просят оказать помощь всех неравнодушных и перевести деньги на указанные реквизиты. Этот вид мошенничества также становится все более популярным.

Фишинг является наиболее опасным и самым распространённым способом мошенничества в интернете. Суть заключается в выманивании у жертвы паролей, пин-кодов, номеров и CVV-кодов. Схем, которые помогают мошенникам получить нужные сведения, очень много.

Так, с помощью спам-рассылок потенциальным жертвам отправляются подложные письма, якобы, от имени легальных организаций, в которых даны указания зайти на «сайт-двойник» такого учреждения и подтвердить пароли, пин-коды и другую информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы. Достаточно распространенным является предложение о работе за границей, уведомление о выигрыше в лотереи, а также сообщения о получении наследства.

Нигерийские письма – также один из самых распространённых видов мошенничества. Типичная схема: жертва получает на свою почту письмо о том, что является счастливым обладателем многомиллионного наследства. Затем мошенники просят у получателя письма помощи в многомиллионных денежных операциях (получение наследства, перевод денег из одной страны в другую), обещая процент от сделки. Если получатель согласится участвовать, то у него постепенно выманиваются деньги якобы на оплату сборов, взяток чиновникам и т.п.

В целом можно сделать вывод о большом количестве разнообразных способов мошенничества в сети интернет. Особенно актуальной данная проблема становится в связи с постоянным увеличением количества пользователей и активным развитием средств интернет-коммуникации, все более плотным внедрением интернета и интернет-платежей в нашу повседневную жизнь.

# **2 РАССЛЕДОВАНИЕ СЛУЧАЕВ ИНТЕРНЕТ-МОШЕННИЧЕСТВА ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ**

Интернет сегодня кроме актуальной и полезной информации содержит потенциально вредные и незаконные сведения, являющиеся благодатной почвой для развертывания противоправной деятельности. Всемирная сеть отличается простотой и дешевизной размещения информации: каждый человек, имея компьютер и подключение к Интернету через провайдера, может создать свой личный сайт или аккаунт в социальной сети, причем установить владельца в большинстве случаев невозможно. Сетевая среда способная влиять на личностные характеристики людей. Виртуальный мир дает дополнительную свободу действий и выражения мыслей, эмоций и чувств, но при этом может легко втянуть в общение маргинальных групп. Для многих людей виртуальная среда иногда кажется даже более привычной, чем реальная. Люди способны довериться совершенно незнакомому человеку (анонимному пользователю Всемирной сети), но могут не принимать во внимание слова не только своих друзей, но родных и близких.

Интернет-мошенничество с одной стороны является результатом эволюции традиционного мошенничества, с другой стороны – это качественно новая группа преступлений, так как при схожести методов реализации, конкретные способы имеют существенные отличия. Данная разновидность преступлений, как и многие другие компьютерные преступления, характеризуется высокой латентностью, во-первых, из-за сложности расследования, а во-вторых, из-за специфики реализации мошеннических схем в Интернете.

Преступления, связанные с мошенническими действиями, описаны в статье 159 УК РФ [2]. Статья 159.6 УК предусматривает ответственность за мошенничество в сфере компьютерной информации, т.е. хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. При этом необходимо учитывать, что преступления, предусмотренные статьями 159.1-159.5 УК РФ (раздел 1.1) также могут совершаться посредством информационных и телекоммуникационных технологий.

## **2.1 Выявление правоохранительными органами мошеннических действий в интернете**

Согласно данным Генеральной прокуратуры Российской Федерации [5], количество киберпреступлений в первом квартале 2020 года выросло на 83,9%, а удельный вес таких деяний достиг 19,9% от общего числа. В основном из-за этого фактора уровень преступности в стране в целом вырос на 4%.

При этом следует держать в голове то, что длительный период граждане практически не обращались с заявлениями в полицию, а также то, что ранее ежегодный прирост киберпреступности был около 70% (рисунок А2).

По мнению экспертов интернет-портала SecurityLab (<https://www.securitylab.ru>), к концу 2020 года число зарегистрированных киберпреступлений может составить около 0,5 млн. Раскрываемость их – не более 23%. Доля в общем числе преступлений по стране – 19%-22%.

Статистические данные Генеральной прокуратуры за 2019 и первую половину 2020 года по количеству преступлений, совершенных с использованием информационно-телекоммуникационных технологий, подтверждают эти выводы (таблица 1).

Таблица 1 – Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации [5]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Период | Количество преступлений, зарегистрированных в отчетный период | Количество предварительно расследованных преступлений в отчетный период | Выявлено лиц, совершивших преступления |
| **Всего преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации** | | | | |
| Российская Федерация | 2019 | 294 409 | 65 238 | 44 158 |
| 01-07.2020 | 272 737 | 53 141 | 36 271 |
| Республика Башкортостан | 2019 | 7 571 | 1 186 | 787 |
| 01-07.2020 | 7 500 | 1 001 | 678 |
| **Всего преступлений, совершенных с использованием или применением сети «Интернет»** | | | | |
| Российская Федерация | 2019 | 157 036 | 35 181 | 20 656 |
| 01-07.2020 | 155 745 | 30 065 | 17 509 |
| Республика Башкортостан | 2019 | 3 686 | 415 | 182 |
| 01-07.2020 | 3 706 | 338 | 121 |
| **Мошенничество** | | | | |
| Российская Федерация | 2019 | 119 903 | 9 798 | 3 556 |
| 01-07.2020 | 109 849 | 7 628 | 2 732 |
| Республика Башкортостан | 2019 | 3 076 | 155 | 55 |
| 01-07.2020 | 2 463 | 88 | 48 |

Аналогичная картина наблюдается и по Республике Башкортостан.

По мнению бывшего следователя, полковника полиции в отставке Бубенновой Любовь Викторовны, количество преступлений, совершаемых через интернет (и особенно связанных с мошенническими действиями), будет только расти в ближайшие годы. Большая проблема, по ее мнению, «стоит со сбором доказательной базы по подобным преступлениям и с нежеланием самих потерпевших обращаться в полицию. Часть потерпевших не считает ущерб значительным для себя, из-за чего и не пишет заявление. Но у преступника таких потерпевших может быть очень много и суммарный ущерб будет колоссальным. Второй случай – безверие в возможности полиции найти преступника, особенно при современном ее уровне в данной области. Все эти причины скорее от безнадежности, а не просто нежелание».

По преступлениям, связанным с мошенничеством с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации статистика расследованных правоохранительными органами дел очень удручающая. В целом по России процент расследованных дел составляет 8,17% за 2019 год и 6,94% за семь месяцев 2020 года. По Республике Башкортостан, соответственно, 5,04% за 2019 год и 3,57% за семь месяцев 2020 года (таблица 1) [5].

Львиная доля уголовных дел по зарегистрированным преступлениям в сфере мошенничества приостановлено по ч. 1 ст. 208 УПК РФ «Основания, порядок и сроки приостановления предварительного следствия» – предварительное следствие приостанавливается при наличии одного из следующих оснований:

1) лицо, подлежащее привлечению в качестве обвиняемого, не установлено;

2) подозреваемый или обвиняемый скрылся от следствия либо место его нахождения не установлено по иным причинам;

3) место нахождения подозреваемого или обвиняемого известно, однако реальная возможность его участия в уголовном деле отсутствует;

4) временное тяжелое заболевание подозреваемого или обвиняемого, удостоверенное медицинским заключением, препятствует его участию в следственных и иных процессуальных действиях.

Как заключают эксперты интернет-портала SecurityLab (<https://www.securitylab.ru>), российским правоохранительным органам не хватает достаточного числа подготовленных в ИТ сотрудников, отсутствуют методики расследования инновационных преступлений, нет надежных и эффективных информационно-аналитических решений. Отсутствует принципиально новая система криминалистического учета и идентификации в киберпространстве, так необходимая нам сегодня [6].

## **2.2 Личность интернет-мошенника**

Одной из характерных особенностей, присущих интернет-преступности, является преобладание преступников мужского пола. Несмотря на то, что среди пользователей Интернета соотношение женщин и мужчин примерно одинаково, последние проявляют более высокую криминальную активность. Преобладание лиц мужского пола среди интернет-преступников, как и в большинстве традиционных преступлений, объясняется исторически сложившимся более высоким уровнем социальной активности мужчин.

Анализируя возраст различных Интернет-преступников, можно отметить, что подавляющее большинство преступленных посягательств совершается лицами в возрасте до 34 лет, причём пик приходится на период примерно с 18 до 30 лет:

1. до 18 лет – 18%;
2. 18-30 лет – 67%;
3. 30-45 лет – 12%;
4. 45 и старше – 3% [7].

Доля учащихся всех уровней составила примерно 64%, что эквивалентно около трети от всей аудитории Интернета (по социальному положению). Таким образом, именно учащиеся и студенты вузов проявляют в Интернете повышенную криминальную активность. Одним из объяснений такого положения вещей является то, что возраст от 20 до 40 лет считается периодом наивысшей активности у большинства людей. Около 18% интернет-преступников имеют среднее специальное образование, т.е. окончили школу, техникум, либо учились на 1-2 курсах институтов. Примерно такое же количество имеют неоконченное высшее образование (в основном, студенты старших курсов вузов). Лишь 9% преступников имеют высшее образование.

Одной из характерных особенностей интернет-преступности вообще и интернет-мошенничества, в частности, является отсутствие судимости (либо совершение преступления впервые) у преступников – около 90% всех случаев. Действительно, если сравнивать мошенничество в сети интернет и обычное мошенничество, то можно увидеть, по сути, две противоположные картины. Однако представляется, что такая тенденция, со временем, пойдёт на убыль. По сравнению с традиционными видами мошенничества интернет- мошенничество является достаточно молодым видом преступления.

Анализ нравственно-правовых характеристик личности интернет-преступников, представленные в работах различных исследователей, показывает, что подследственные, так или иначе, признавали свою вину полностью или частично.

Представляется, что подобное поведение складывается в результате взаимодействия следующих обстоятельств:

1) страх перед правоохранительными органами, частично связанный с отсутствием опыта общения с ними (как было отмечено выше, практически все осуждённые совершали преступление впервые);

2) следы доведенных до окончания расследования интернет-преступлений вообще и мошенничеств, в частности, были плохо скрыты, как следствие, доказательство вины частично облегчено. Поэтому задержанные, понимая, что запутать следствие либо иными способами снять с себя обвинение они не в состоянии, соглашаются на сотрудничество.

Существует также определённый набор особенностей личности, обуславливающих выбор конкретной преступной деятельности, которую мошенник собирается осуществлять.

Среди социально-психологических признаков личности, исследователи [7] указывают следующие:

1. Глубокие познания в различных областях человеческой деятельности.

2. Определяющий мотив преступления – корысть. Соотнося данную характеристику с примерным возрастом типичного интернет- мошенника (примерно 18-30 лет, причём основной процент будет приходиться на период с 18 до 25 лет), можно заключить, что типичный интернет-мошенник - учащийся вуза или учреждения среднего профессионального образования, не работающий и, возможно, находящийся на иждивении родителей или других родственников.

3. Хорошие коммуникативные качества, изобретательность, наблюдательность. В практике расследования мошенничеств в сети интернет известны случаи, когда преступники успешно общались со своими жертвами от имени женщин, будучи при этом мужчинами (такие случаи встречаются, в основном, в брачных аферах с использованием сайтов знакомств).

От характерных особенностей личности типичного интернет- мошенника во многом зависит тот вид мошенничества, на котором он специализируется.

Следует отметить, что интернет-мошенник планирует именно незаконную деятельность и именно в Интернете, руководствуясь, в большинстве случаев, соображениями рациональности, а не уровнем своих знаний в области информационных технологий или привязанности к компьютерам, что более свойственно таким преступлениям, как неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ).

В некоторых случаях одним из важных качеств личности Интернет- мошенника является наличие организаторских способностей. Дело в том, что некоторые виды Интернет-мошенничества являются технически сложными в плане исполнения, поэтому в их совершении принимают участие несколько человек. В такой ситуации залогом успешной реализации поставленной задачи будут чётко распределённые роли и постоянный контроль. Распределение ролей в группе обусловливает также различие набора личностных качеств каждого её члена. Примером такого разделения можно считать мошенничество в брачной сфере. При совершении данного преступления группой, очевидно, что, например, коммуникативные качества более важны непосредственным исполнителям (это лица, которые непосредственно занимаются перепиской с жертвами), чем организатору.

# **3 ПРЕДОТВРАЩЕНИЕ ИНТЕРНЕТ-МОШЕННИЧЕСТВА**

Основное правило защиты от интернет-мошенничества простое: если что-то в Сети звучит слишком хорошо, чтобы быть правдой, это, вероятно, обман.

Многие эксперты по интернет-безопасности предупреждают, что вы никогда не должны нажимать на ссылки в электронных письмах и точка. Желательно никогда не нажимать на любые ссылки, которые могут вести на мошеннические (фишинговые) сайты или на зараженные веб-ресурсы. Помните, что хакеры и мошенники могут подделывать сообщения, чтобы они выглядели так, как будто они получены из источников, которым вы доверяете, но на самом деле такие ссылки могут вести на фальшивые веб-сайты, предназначенные для сбора вашей личной информации, а также для загрузки на ваше устройство вредоносной программы. Часто при переходе по таким фишинговым ссылкам на ваше устройство автоматически устанавливается вредоносная программа.

Этот совет особенно актуален, когда дело доходит до сообщений от ваших финансовых учреждений. Законные банки и такие сервисы, как Яндекс Деньги, обычно не просят вас подтвердить свои данные, перейдя по ссылке. Да, иногда банки и платежные системы могут присылать вам на почту рекламные предложения или информацию о сбросе пароля (если вы сами на их сайте запрашивали это). Если вы получили такое уведомление и не помните, что запрашивали его, игнорируйте письмо. Если финансовое учреждение прислало вам письмо, для прочтения которого нужно зайти в личный кабинет, никогда не переходите по ссылке в письме. Для этого откройте веб-браузер или приложение на смартфоне и войдите в свою учетную запись обычным способом. Зайдя в кабинет, проверьте в системе входящее личное сообщение (если оно, конечно, существует).

Также, прежде чем войти на сайт банка или другого финансового учреждения, потратьте секунду на поиск на экране значка защищенного соединения (как правило, это иконка замка). Хотя это, конечно, и не надежный способ отличить фальшивый сайт от реального, по крайней мере, он дает вам немного дополнительной информации о том, что на сайте используется зашифрованое соединение с сайтом или службой, что делает сайт (потенциально) более легитимным. Хотя имейте в виду, что в последнее время участились случаи, когда мошенники в Сети стали все чаще использовать для фишинговых сайтов защищенный протокол (HTTPS).

*Не выдавайте свои пароли.*

Это очевидно, но менее опытные люди могут раскрыть случайно свои пароли. Особенно если их запрос кажется законным. Жесткое и главное правило заключается в том, что вы никогда не должны выдавать свои пароли никому. Даже если вас об этом просит сотрудник банка. Пароль – это не то, что люди или компании должны у вас когда-либо просить напрямую. Это все равно что люди попросят у вас ключ от вашей квартиры или машины. Если по какой-либо причине вы получите электронное письмо или текстовое сообщение с просьбой отправить пароль, не делайте этого. И неважно, кто прислал письмо. Хоть об этом вас просят в письме сам президент или ФСБ.

*Используйте надежные пароли (и секретные вопросы).*

Многие люди до сих пор используют глупые легкие пароли, такие как «пароль» и «123456». Не будьте одним из них. Если ваш пароль легко угадать (поскольку он содержит основную идентификационную информацию, такую ​​как дата вашего рождения или имя вашего супруга), даже не имеет значения, раскроете ли вы его кому-то. Хакер взломает простой пароль в кратчайшие сроки.

Если вы используете один и тот же пароль для всего и этот пароль становится утечкой во время взлома данных, все ваше онлайн-существование будет раскрыто. Мы рекомендуем использовать менеджер паролей для отслеживания ваших десятков или сотен уникальных логинов. Например, отлично зарекомендовал себя менеджер паролей Касперский, который поможет вам в одной программе объединить все логины и пароли. Причем храниться они будут в защищенном облаке, которым вы сможете пользоваться с любого устройства, синхронизируя данные между ними.

Слабым звеном в вашей безопасности могут быть те секретные вопросы и ответы, которые большинство сайтов просят вас ввести, чтобы помочь вам сбросить пароль. Даже если ваш пароль надежный, ваш секретный вопрос/ответ часто может быть очень легким. Поэтому вы должны обязательно защитить свои учетные записи с помощью сложных секретных вопросов/ответов. И по возможности используйте двухфакторную аутентификацию, чтобы помешать кому-либо получить доступ к вашей учетной записи, даже если у злоумышленников есть ваши учетные данные для входа в личный кабинет банка, онлайн-сервиса, платежной системы, в учетную запись сайта Госуслуги и т. п.

*РЕКЛАМА*

Не покупайте ничего по случайному электронному письму, которое вы получите. Хороший спам-фильтр должен улавливать очевидные вещи, такие как электронные письма, пытающиеся продать вам все: от дешевых часов до поддельных товаров для улучшения здоровья. Но мошенникам относительно легко притвориться, что они интернет-магазин Ozon, AliExpress и т. д. То есть точно так же, как им легко притвориться, что они из вашего банка.

Самое простое правило – никогда ничего не покупать по электронной почте. Возможно, вы можете сделать исключение для новостных рассылок по электронной почте с сайтов, которым вы доверяете, но, по крайней мере, убедитесь, что вы ничего не нажимаете в письмах. Вы всегда можете перейти непосредственно на Ozon или в любой интересующий вас интернет-магазин, введя этот адрес прямо в панели интернет-браузера, и найти продукт, который они вам рекламируют.

Будьте настороже, когда получаете предложения о работе, которые выглядят слишком хорошими, чтобы быть правдой

Если вы ищете работу или просто способ заработать дополнительные деньги, очень скептически относитесь к предложениям, поступаемым вам на электронную почту. Особенно если вы разместили свое резюме на таких сайтах, как «Из рук в руки» или «Avito». Не то чтобы эти сайты не подходят для поиска работы/подработки, но вы должны быть предельно осторожны, поскольку на этих площадках очень много мошенников, которые ищут доверчивых людей среди соискателей работы.

Если вам приходит предложение «заработать 1000 рублей в час» или «хотим предложить вам работу тайным покупателем – оплата 5000 рублей в день!» и письмо, в котором вам обещают кучу денег почти без работы, будьте уверены, эти предложения полностью фальшивы. Скорее всего, вас хотят одурачить.

Больше всего вас должна насторожить любая работа, включающая выплату через систему электронных платежей Western Union, WebMoney, через другие электронные переводы, денежные переводы или договоры с любой неофициальной денежной выплатой. Иногда мошенники пишут массовые сообщения, что якобы по ошибке положили на счет мобильного телефона или на вашу банковскую карту деньги, даже прикрепляя фотографии со сканом платежных документов.

Таким образом, основной способ защититься от интернет-мошенников заключается в следующем: руководствуйтесь здравым смыслом, когда рассматриваете то, что вам предлагают в Сети или по электронной почте. Согласитесь, когда вам в Интернете сообщают, что вы выиграли в какую-то национальную лотерею, это выглядит смешно и обманчиво, особенно если учитывать, что вы даже не знали, что у вас есть лотерейный билет.

# **ЗАКЛЮЧЕНИЕ**

С развитием человеческого общества, появлением прогрессивных технических возможностей, научных открытий и изобретений, к сожалению, все чаще выявляются новые виды мошеннических действий, которые в последнее время активно совершенствуются. Особенно активный рост мошеннических действий можно наблюдать в сети Интернет. Соответственно, растут и финансовые потери людей от действий преступников. За последние 5 лет количество подобных преступлений выросло в 5 раз. За прошедшие месяцы 2020 года количество преступлений в интернете практически равно их количеству за весь предыдущий год.

По мнению ряда экспертов, а также по результатам анализа статистики совершенных и расследованных преступлений в сети интернет можно сделать вывод об острой необходимости улучшения эффективности действий правоохранительных органов в области расследования случаев интернет-мошенничества. В целом по России процент расследованных дел в области интернет-мошенничества составляет 8,17% за 2019 год и 6,94% за семь месяцев 2020 года. По Республике Башкортостан, соответственно, 5,04% за 2019 год и 3,57% за семь месяцев 2020 года. Львиная доля уголовных дел по зарегистрированным преступлениям в сфере мошенничества в настоящее время приостанавливается в связи с тем, что совершившие преступления лица не установлены.

Как заключает ряд экспертов, российским правоохранительным органам не хватает достаточного числа подготовленных в сфере ИТ сотрудников, отсутствуют методики расследования инновационных преступлений, нет надежных и эффективных информационно-аналитических решений. Отсутствует принципиально новая система криминалистического учета и идентификации в киберпространстве, так необходимая нам сегодня [6].

# **СПИСОК ЛИТЕРАТУРЫ**

1. Число дел о мошенничестве рекордно выросло на фоне пандемии. // <https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9dhttps://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d>
2. Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 31.07.2020)
3. Ильина, Н. Знак доверия: россияне стали в 10 раз чаще кликать на сайты мошенников. Обманывая граждан, злоумышленники активно эксплуатируют тему коронавируса. / Известия, 6 мая 2020. // <https://iz.ru/1007653/natalia-ilina/znak-doveriia-rossiiane-stali-v-10-raz-chashche-klikat-na-saity-moshennikov>
4. Состояние преступности в России за январь - июнь 2020 года. Сборник результатов статистических наблюдений. – М.: Генеральная прокуратура Российской Федерации. Главное управление правовой статистики и информационных технологий, 2020. – 52 с.
5. Генеральная прокуратура Российской Федерации. Портал правовой статистики // <http://crimestat.ru/>
6. Очередной скачок киберпреступности в 2020 году. 19 Апреля, 2020 // <https://www.securitylab.ru/blog/company/CABIS/348156.php>
7. Ермолович, Д.В., Широких, С.В. Некоторые поисковые социально-психологические признаки личности мошенника // <http://www.law.edu.nl/article/article.asp7articleIDH313226>
8. Ревякин С.В. Профилактика мошенничества с использованием современных электронных средств коммуникации / Виктимология 3(17), 2018. – с. 74-80
9. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 31.07.2020)

# **Приложение А. Статистические данные**



Рисунок А1 – Доля случаев мошенничества через интернет и по телефону в России

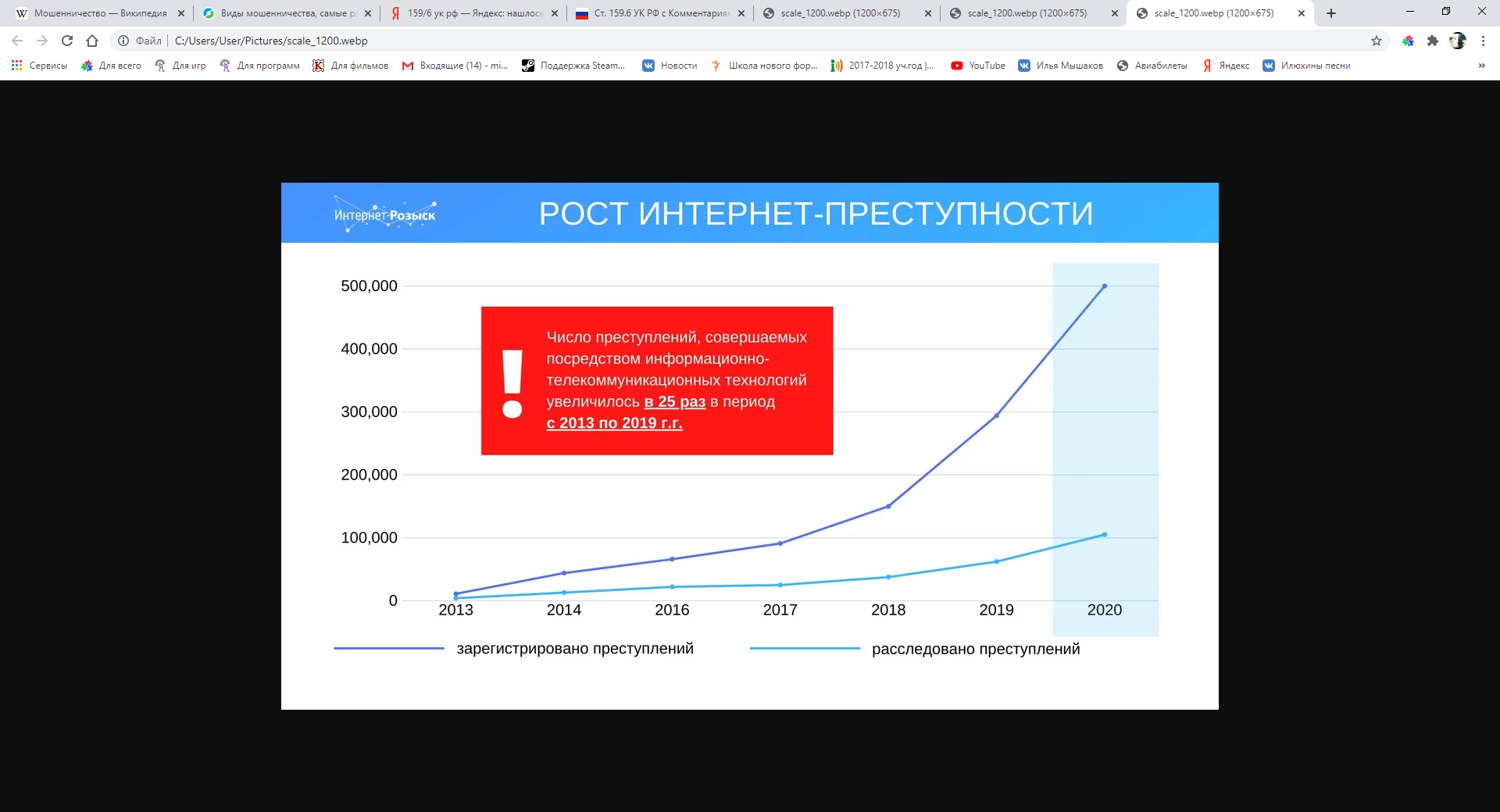


Рисунок А2 – Статистика роста преступлений, совершаемых через интернет и прогноз на 2020 год [6]

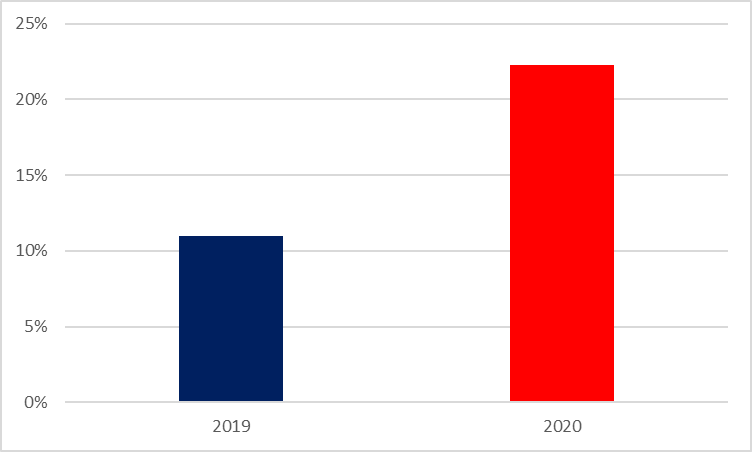


Рисунок А3 – Рост количества преступлений, совершенных с использованием информационно-телекоммуникационных технологий, из общего числа преступлений

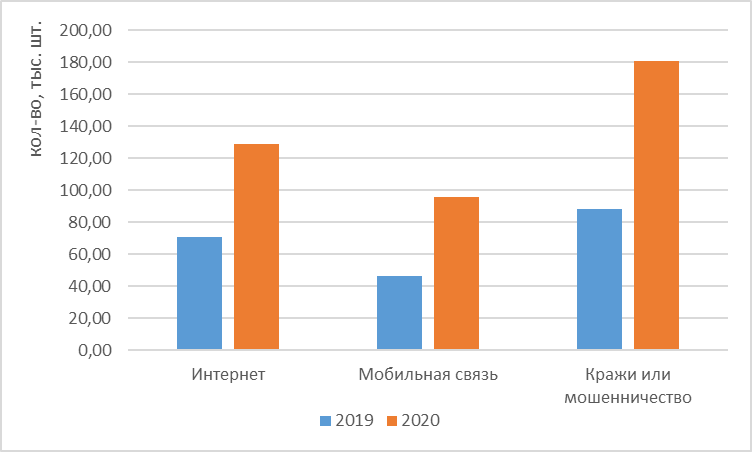


Рисунок А4 – Количество «киберпреступлений», совершаемых через интернет или посредством мобильной связи и классифицируемых, как мошенничество или кража



Рисунок А5 – Количество случаев мошенничества за период самоизоляции (апрель-июнь 2020 г.) по сравнению с аналогичными периодами прошлых лет [1]