УДК 343 **DOI: 10.34670/AR.2021.84.47.027**

Особенности квалификации и современные способы совершения мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ)

Абдульмянова Татьяна Владимировна

Кандидат исторических наук,
доцент кафедры уголовного права и криминологии,
Саранский кооперативный институт (филиал),
Российский университет кооперации,
430027, Российская Федерация, Саранск, ул. Транспортная, 17;
e-mail: abdulmyanova.tanya@mail.ru

Аннотация

Развитие информационно-телекоммуникационных технологий облегчило и ускорило совершение многих действий в повседневной жизни, в том числе связанных с осуществлением финансовых операций. Сегодня большое количество людей отдают предпочтение безналичной форме денежных расчетов, используя платежные карты ввиду быстроты совершения операций и удобства использования. Наряду с этим электронные средства платежа являются объектом внимания и злоумышленников, которые из года в год разрабатывают и совершенствуют способы совершения мошеннических действий в отношении денежных средств граждан, находящихся на платежных картах. В данной статье анализируются особенности специального вида мошенничества, закрепленного в ст. 159.6 УК РФ, выявляются особенности состава данного преступления, рассматриваются вопросы квалификации данного преступления. Приводятся примеры судебной практики привлечения к уголовной ответственности за преступление, предусмотренное ст. 159.6 УК РФ. Особое внимание уделяется рассмотрению современных способов совершения мошенничества в сфере компьютерной информации, которые на данный момент распространены в преступной практике.

Для цитирования в научных исследованиях

Абдульмянова Т.В. Особенности квалификации и современные способы совершения мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) // Вопросы российского и международного права. 2021. Том 11. № 6А. С. 133-141. DOI: 10.34670/AR.2021.84.47.027

Ключевые слова

Уголовное право, преступление, квалификация преступлений, защита собственности, мошенничество, виды мошенничества, интернет-мошенничество, уголовная ответственность, уголовное наказание, санкции.

Введение

Учитывая данные о количестве обращений граждан, подвергшихся противоправным действиям в сети Интернет, растущей технической и юридической грамотности преступников, можно прийти к неутешительному выводу о том, что мер противодействия мошенничеству в сети Интернет недостаточно. Укрепление современной законодательной базы, регулирующей деятельность организаций по пресечению подобного рода угроз, на наш взгляд, должно сопровождаться закреплением на государственном уровне общественного аппарата по контролю за противоправной информацией в сети Интернет.

Так как большинство мошеннических сайтов расположены не на российских хостингах и финансовые операции по ним проводятся за пределами территории, где распространяется российское законодательство, на данный момент единственным оперативным решением может быть лишь блокировка подобных сайтов без решения суда. Судебные разбирательства могут продлеваться во времени, в то время как преступная деятельность будет продолжаться, тем самым ослабляя экономическую безопасность государства.

На данный момент уже введена подобная практика в отношении сайтов, содержащих контент экстремистского характера, например призывы к массовым беспорядкам, информационные материалы организаций, нежелательных на территории РФ и т. д. Стоит учитывать, что предоставление подобных полномочий несет за собой массу рисков, поскольку возможны не только ошибочные блокировки, но и преднамеренное устранение и блокировка не представляющих угрозу сайтов, порталов и аккаунтов в социальных сетях. Недобросовестное использование подобных полномочий при недобросовестной конкурентной борьбе в любых сферах бизнеса и оказания государственных услуг, с учетом человеческого фактора, может нанести серьезный ущерб экономике страны.

Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ): характеристика состава преступления

Экономическая безопасность как сложная категория может быть обеспечена различными формами практической деятельности человека. В частности, к ним можно отнести законотворческую и правоприменительную форму.

Федеральным законом от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» УК РФ дополнен нормой об ответственности за мошенничество в сфере компьютерной информации. Под мошенничеством в сфере компьютерной информации понимается 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 [Уголовное право…, 2019, 45].

Видовым объектом преступления являются социально значимые интересы и отношения в сфере охраны собственности. Непосредственным объектом мошенничества выступают социально значимые интересы и отношения в сфере охраны конкретной формы собственности. Предметом преступления становится чужое имущество, хищение или приобретение права на которое осуществляется путем ввода, удаления, блокирования, модификации компьютерной

информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Объективная сторона мошенничества в сфере компьютерной информации выражается в хищении чужого имущества, равно как и в приобретении права на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Преступление признается оконченным с момента получения виновным суммы денег (чужого имущества), равно как и приобретения им юридического права на распоряжение такими деньгами (имуществом). Так, в Мотовилихинском районе Перми состоялся суд над местным жителем 1993 г. рождения. Он признан виновным в совершении одиннадцати преступлений, предусмотренных ч. 2 ст. 272 УК РФ (неправомерный доступ к компьютерной информации), пяти преступлениях, предусмотренных ч. 1 и ч. 2 ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации), и двух покушениях на мошенничество в сфере компьютерной информации. Как установило следствие, в мае 2017 г., располагая неправомерным доступом к охраняемой законом компьютерной информации, он модифицировал данные пользователей популярного интернет-магазина, на личных счетах которых имелись денежные средства. Их можно было использовать на приобретение различных товаров. В результате информация о заказе приходила на его электронную почту, а не к истинному владельцу аккаунта. Таким образом, осужденный практически через день заказывал товары в интернет-магазине, что-то для себя, что-то на перепродажу. Некоторые покупки отменяли по причине отсутствия товара у поставщика, а денежные средства возвращали пользователю, однако злоумышленника этот факт не останавливал. Он формировал новый заказ на приобретение вещей. Другие запросы на товар аннулировались сотрудниками сайта из-за подозрения в несанкционированном доступе. Некоторые пользователи сами выявляли взлом, когда не могли получить доступ к учетной записи. Граждане немедленно обращались в клиентский центр, а заказы интернет-преступника также аннулировались [В Перми…, www].

Субъективную сторону мошенничества в сфере компьютерной информации образует прямой умысел на завладение чужим имуществом посредством незаконного вторжения в функционирование средств компьютерной информации. Так, прокуратура Тюменской области направила в Центральный районный суд Тюмени уголовное дело в отношении 31-летнего жителя Перми за хищение более 10,5 млн руб. Он обвиняется по ч. 4 ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации, совершенное группой лиц по предварительном сговору, с банковского счета, в особо крупном размере), и ему грозит лишение свободы на срок до 10 лет. Следствие установило, что в мае 2020 г. обвиняемый совместно с неустановленным лицом реализовал план по хищению крупной денежной суммы у строительной фирмы в Ялуторовске (Тюменская область). Они отправили на электронную почту застройщика вредоносную компьютерную программу. С ее помощью мошенники получили удаленный доступ к расчетному счету организации и под видом зарплаты перевели на свои банковские карты более 10,5 млн руб. Согласно договоренности, мужчина вывел деньги в банкоматах Краснодара, из которых оставил себе 300 тыс. руб., а остальные средства были переведены в биткоины. В ходе розыска он был задержан краснодарской полицией и заключен под стражу по решению суда. Обвиняемый в ходе следствия вернул организации больше, чем похитил (11,9 млн руб.). Уголовное дело в отношении соучастника выделено в отдельное производство. Ранее суд в Омске назначил штраф разработчику вредоносных программ,

получающих доступ к номерам банковских карт, адресам электронных почт и аккаунтам различных сервисов для получения незаконной выгоды [В Тюмени…, www].

Субъектом преступления признается вменяемое физическое лицо, достигшее 16 лет.

Классификация современных способов интернет-мошенничества

Современная преступность ежедневно подвергается изменениям, появляются новые способы совершения противозаконных действий, меняется сфера концентрации преступного контингента.

Проанализировав статистические данные, размещенные на сайте МВД России, можно отметить, что недавно стали выделять сведения о преступлениях, совершаемых в информационно-телекоммуникационной среде. Это подтверждает масштабный рост рассматриваемой преступности и ее негативное воздействие на общественные отношения.

Действительно, значительная часть населения в данный период проводит время в сети Интернет как в развлекательных целях, так и с целью заработка, так как многие предприятия, учреждения, общественные места работают в ограниченном режиме или вовсе закрыты. Количество пользователей в Интернете повышается, онлайн-пространство начинает осваивать даже самое возрастное поколение. Мошенники используют эту непростую ситуацию, осваивая новые способы дистанционного хищения персональных данных или денежных средств с банковских карт граждан [Мальченкова, Мальченков, Сологубов, 2021, 24-26].

Рассмотрим наиболее распространенные способы интернет-мошенничества, т. е. незаконного овладения чужими средствами или данными, являющимися собственностью правообладателя.

Можно предложить следующую современную классификацию способов интернет-мошенничества [Борсученко, Амосов, 2020].

1. Фиктивные интернет-магазины – довольно распространенный вид мошенничества, представленный сайтами-одностраничниками с уникальным ценовым предложением на какой-либо товар. Как правило, фиктивные интернет-магазины работают по частичной либо стопроцентной предоплате. Соответственно, жертва, осуществив перевод денежных средств, не получает товар. Далее сайт блокируется и со временем «переезжает» на другой хостинг либо меняет доменное имя и продолжает свою противоправную деятельность. Такой сайт может быть наполнен большим количеством фальшивых отзывов с целью создания образа добропорядочного интернет-магазина и введения в заблуждение потенциальных жертв. Такой вид мошенничества является одним из самых простых методов осуществления преступной деятельности в сети Интернет и наносит большой урон по финансовой состоятельности слабозащищенных и неосведомленных граждан с учетом низкого уровня их информационной грамотности.

2. Фишинг (англ. phishing от fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей. Для получения конфиденциальной информации (персональных данных пользователей, паролей, данных кредитных и дебетовых карт и т. д.) часто используется следующая схема: создание поддельного сайта – введение в заблуждение, обман жертвы – получение доступа к конфиденциальной информации.

Мошенники рассылают на электронную почту сообщения, идентичные сообщениям известной и надежной организации либо контакта. Рассылки в основном осуществляются с

помощью спуфинга – изменения адреса отправителя, отображаемого у получателя письма. Атака выполняется с помощью вредоносного файла, прикрепленного в сообщении и содержащего фишинговое программное обеспечение, а также посредством ссылок, вследствие перехода по которым пользователь попадает на вредоносный веб-сайт. Происходит заражение компьютера, смартфона или иного гаджета, и мошенник получает всю необходимую информацию для последующего хищения денежных средств. Перейти по этой ссылке жертве предлагается под разными предлогами, вариантов обмана множество. Например, мошенниками практикуются рассылки электронных писем от имени крупных банков, в которых сообщается, в частности, об изменениях в системе безопасности, блокировки банковской карты держателя или попытки хищения денежных средств с нее. Номер карты, ПИН-код, CVV/CVC – объекты интересов злоумышленников, и часто пользователи, введенные в заблуждение и/или напуганные, предоставляют им эту информацию.

При переходе на сайт «банка» жертва вводит персональные данные, тем самым открывая преступникам доступ к конфиденциальным сведениям и возможности с их помощью совершить противоправные действия. С помощью фишингового программного обеспечения, установленного на компьютер или гаджет «клиента» фишера, возможно перенаправление при открытии определенных приложений или сайтов на сайт-двойник, где кража интересующей мошенника информации зачастую происходит в автоматическом режиме. Также излюбленной технологией мошенников является копирование сайтов известных интернет-магазинов, где совершение «покупки» чревато тем, что данные банковской карты получает мошенник, который снимает с нее все имеющиеся средства [Крюкова, Алимамедов, 2021].

3. Еще одним способом завладения денежными средствами с платежных карт посредством сервисов связи является смишинг. Данный способ, безусловно, имеет общие черты с фишингом и фармингом, но вредоносная ссылка направляется пользователям через SMS-сообщения. Такое сообщение может иметь вид SMS от известного банка или иной компании. Как правило, смишинг-сообщения небольшие по размеру. Злоумышленники специально сообщают минимум информации потенциальным жертвам, поясняя, что более подробную справку возможно получить при переходе по ссылке. Далее лицо перенаправляется на сайт, схожий по дизайну с популярными веб-страницами. Нередко на таких сайтах размещаются логотипы банковских компаний, действительные номера телефонов для того, чтобы не вызвать сомнений у потенциальной жертвы. На таких сайтах лицо вводит персональные данные, а преступники, используя эту информацию, завладевают денежными средствами [Джусь, 2021].

4. Черный инфобизнес – популярный вид интернет-мошенничества с конца 2017 г. Стоит отметить, что сам по себе инфобизнес не является мошенничеством, поскольку представляет собой продажу информации в форме книг, аудио- и видеофайлов, презентаций и т. п. Однако со стремительным развитием инфобизнеса в последние годы появился и его мошеннический аналог. Под видом вебинаров, курсов повышения квалификации либо онлайн-школ пользователю предполагают купить информацию либо менторство и наставничество на определенный срок в какой-либо сфере бизнеса или науки. Однако после перечисления средств пользователь в лучшем случае получает информацию, которую можно найти в сети Интернет в свободном доступе либо, не получив блага или услуги, теряет свои денежные средства [Сергеев, Любименко, Савватеева, 2020].

5. Мошенничество с распространением контента представляет собой вид мошенничества, при котором мошенниками создается архив с нужной пользователю информацией. Как правило, срабатывает несложный скрипт, подменяющий название архива на информацию,

запрашиваемую пользователем в поисковой системе. При попытке распаковки либо загрузки данного архива пользователю предлагается отправить сообщение для верификации его аккаунта, вследствие чего с его счета списывается крупная сумма денежных средств, а искомую информацию он так и не получает.

6. Финансовые пирамиды законодательно запрещены на территории Российской Федерации, независимо от того, являются ли они традиционными финансовыми пирамидами либо интернет-проектами. Несмотря на то, что за организацию финансовых пирамид установлена уголовная ответственность, они являются весьма распространенным видом мошенничества в сети Интернет, а реклама подобных проектов широко распространена в социальных сетях. Стоит учесть, что, помимо традиционных интернет-пирамид вида МММ, довольно распространены компании, работающие по принципу MLM. Это многоуровневый/сетевой маркетинг. Концепцией MLM является реализация товаров и услуг, которая основана на создании сети независимых дистрибьюторов (сбытовых агентов), каждый из которых, помимо сбыта продукции, также обладает правом на привлечение партнеров, имеющих аналогичные права. При этом доход каждого участника сети состоит из комиссионных за реализацию продукции и дополнительных вознаграждений (бонусов), зависящих от объема продаж, совершенных привлеченными ими сбытовыми агентам. Сама по себе концепция сетевого маркетинга не является мошенничеством, и многие крупные компании, такие как «Орифлейм», «Avon», ведут бизнес, основываясь на данной схеме. Однако в сети Интернет работают компании, которые продают товар крайне сомнительного качества, который впоследствии дистрибьютор просто не может реализовать, либо прикрываются схемой MLM и оказывают фиктивные финансовые услуги.

7. Интернет-казино и нелегальные букмекеры – это противоправный вид интернет-мошенничества, представляющий, на наш взгляд, наибольшую угрозу экономической безопасности государства. Законодательно онлайн-казино запрещены, что регулируется Федеральным законом от 29 декабря 2006 г. № 244-ФЗ, согласно которому деятельность по организации и проведению азартных игр с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, а также средств связи, в том числе подвижной связи, запрещена.

Проблема регулирования казино в сети Интернет состоит в том, что в 90% случаев компании, владеющие данными ресурсами, зарегистрированы в офшорных зонах, соответственно, привлечение их к ответственности является невозможным. Методом борьбы в данном случае является лишь блокировка данного ресурса на территории Российской Федерации, но этот процесс не является быстрым, так как для подобного решения реализуется следующая цепочка действий: от конкретного лица должно последовать обращение о защите своих потребительских прав в отделение Роскомнадзора, который осуществит блокировку подобного сайта, но только в соответствии с вынесенным решением суда. Такая мера на практике будет неэффективна, поскольку компании, ведущие подобного рода деятельность, во-первых, обладают финансовыми возможностями коррупционного свойства, во-вторых, в случае блокировки сайта переходят на другой подобный сайт, в-третьих, даже в случае введения непрерывного мониторинга подобного контента, помимо самого игорного сайта, компании наполняют сеть агрессивной рекламой заработка на казино и букмекерских ставках.

Важно отметить, что главной особенностью способов совершения таких видов мошенничеств является отсутствие непосредственного визуального контакта между потерпевшим и преступником. Этот фактор существенно влияет на оперативность проведения

следственных действий. Таким образом, мы перечислили лишь некоторые способы совершения мошеннических действий. В практической деятельности сотрудники правоохранительных органов сталкиваются все с новыми и новыми схемами, в связи с чем необходимо постоянно совершенствовать свои знания в данной сфере.

Можно также сказать о том, что как правовое, так и техническое регулирование противоправных действий в телекоммуникационных сетях попадает в безвыходную ситуацию. Выходом из сложившейся ситуации могут стать совершенствование законодательной базы, регулирующей подобные ресурсы, и организация открытой дискуссии юристов, экономистов, технических специалистов и органов управления с целью нахождения вариантов решения данной проблемы [Потапова, 2020].

Заключение

В настоящее время технический прогресс не стоит на месте. В данный момент значительное место занимают цифровые технологии, которые вошли в повседневную жизнь человека, используются для государственного функционирования, ведения бизнеса и т. д. Мошенничество идет в ногу со временем, изобретаются новые преступные схемы, и цифровые технологии являются инструментом для хищения чужого имущества.

В современном мире Интернет играет практически ключевую роль, наблюдается тенденция его превращения в альтернативу обычной жизнедеятельности общества. С помощью Интернета происходит беспрепятственное общение, совершаются покупки, реализуется дистанционное образование. Интернет стал рыночной площадкой, обширной сферой электронного бизнеса, а также резервуаром для хранения значительных объемов конфиденциальных данных, в том числе финансовых и персональных.

Пропорционально числу пользователей растет и количество мошеннических действий, совершаемых во Всемирной паутине. Интернет-мошенники – это преступники новой градации, хорошо оснащенные, технически грамотные и обезличенные, что является неблагоприятным фактором в практике расследований. По оценкам Интерпола, темпы роста преступности с использованием Интернета являются самыми быстрыми на планете.

Решение актуальных проблем, связанных с мошеннической деятельностью в сети Интернет, должно быть одним из первостепенных и безотлагательных вопросов на повестке современного аппарата управления государством. Требуются не только совершенствование и модернизация современного законодательства, регулирующего деятельность в Сети, но и наращивание технических мощностей, а также привлечение специалистов смежных областей для диалога и поиска возможных решений и путей нивелирования угроз, встающих перед государством в связи с возрастающей активностью мошенников в Интернете. Следует выстроить полноценное взаимодействие специалистов в области юриспруденции, управления и технологического обеспечения путем формирования площадок для их совместной работы. Создание обособленного подразделения необходимо, но и гражданам нужно быть бдительнее и внимательнее относиться к своей информационной безопасности в онлайн-среде.

Библиография

1. Борсученко С.А., Амосов Е.А. Мошенничество в сфере компьютерной информации: вопросы теории и практики // Цифровизация рыночных отношений: вопросы экономики и права. М., 2020. С. 3-9.
2. В Перми вынесен приговор виновному в серии преступлений в сфере телекоммуникаций и компьютерной информации. URL: https://59.xn--b1aew.xn--p1ai/news/item/15783318

3. В Тюмени будут судить жителя Перми за хищение 10,5 млн рублей с помощью вирусного ПО. URL: https://www.kommersant.ru/doc/4637386
4. Джусь А.С. О некоторых способах совершения мошеннических действий в отношении денежных средств граждан, находящихся на платежных картах // Материалы XVIII Международной научной конференции студентов «Сибирские юридические студенческие чтения». Омск, 2021. С. 204-207.
5. Крюкова И.В., Алимамедов Э.Н. Фишинг как вид интернет-мошенничества // Наукосфера. 2021. № 2-2. С. 196-201.
6. Мальченкова В.В., Мальченков Е.В., Сологубов А.Ю. Мошенничество как социально-правовое явление // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2021. № 21-2. С. 24-26.
7. О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации: федер. закон Рос. Федерации от 29.12.2006 № 244-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 20.12.2006: одобр. Советом Федерации Федер. Собр. Рос. Федерации 27.12.2006. URL: http://www.consultant.ru/document/cons_doc_LAW_64924/
8. Потапова А.В. Мошенничество в сети интернет: криминологическая характеристика и проблемы квалификации // StudNet. 2020. Т. 3. № 6. С. 52-57.
9. Сергеев Д.Р., Любименко О.А., Савватеева О.В. Мошенничество в сети интернет как угроза экономической безопасности государства // Теоретическая экономика. 2020. № 3. С. 76-84.
10. Уголовное право в понятиях и терминах. Саранск, 2019. 80 с.
11. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13.06.1996 № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24.05.1996: одобр. Советом Федерации Федер. Собр. Рос. Федерации 05.06.1996. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/

The features of legal assessment and modern methods of committing fraud in the field of computer information (Article 159.6 of the Criminal Code of the Russian Federation)

Tat'yana V. Abdul'myanova

PhD in History,
Associate Professor at the Department of criminal law and criminology,
Saransk Cooperative Institute (branch),
Russian University of Cooperation,
430027, 17, Transportnaya st., Saransk, Russian Federation;
e-mail: abdulmyanova.tanya@mail.ru

Abstract

The article points out that the development of information and telecommunication technologies facilitated and accelerated the performance of many actions in everyday life, including those related to the implementation of financial transactions. Today, a large number of people prefer the non-cash form of payments using payment cards due to the speed of transactions and ease of use. The article emphasizes that electronic means of payment are also the object of attention of cybercriminals, who from year to year develop and improve methods of committing fraudulent actions in relation to the funds of citizens that are on payment cards. The author of the article makes an attempt to examine and analyze the features of the special type of fraud, enshrined in Article 159.6 of the Criminal Code of the Russian Federation. The article aims to identify the features of this crime and to consider some issues of its legal assessment. It also deals with the judicial practice of bringing people to criminal liability under Article 159.6 of the Criminal Code of the Russian Federation. Special attention is paid to the consideration of some modern methods of committing fraud in the field of computer information, which are currently common in criminal practice.

For citation

Abdul'myanova T.V. (2021) Osobennosti kvalifikatsii i sovremennye sposoby sovershenіya moshennichestva v sfere komp'yuternoi informatsii (st. 159.6 UK RF) [The features of legal assessment and modern methods of committing fraud in the field of computer information (Article 159.6 of the Criminal Code of the Russian Federation)]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 11 (6A), pp. 133-141. DOI: 10.34670/AR.2021.84.47.027

Keywords

Criminal law, crime, legal assessment, property protection, fraud, types of fraud, Internet fraud, criminal liability, criminal punishment, sanctions.

References

1. Borsuchenko S.A., Amosov E.A. (2020) Moshennichestvo v sfere komp'yuternoi informatsii: voprosy teorii i praktiki [Fraud in the field of computer information: the issues of theory and practice]. In: *Tsifrovizatsiya rynochnykh otnoshenii: voprosy ekonomiki i prava* [The digitalization of market relations: economic and legal issues]. Moscow, pp. 3-9.
2. Dzhus' A.S. (2021) O nekotorykh sposobakh sovershenіya moshennicheskikh deistvii v otnoshenii denezhnykh sredstv grazhdan, nakhodyashchikhsya na platezhnykh kartakh [On some ways of committing fraudulent actions in relation to the funds of citizens that are on payment cards]. *Materialy XVIII Mezhdunarodnoi nauchnoi konferentsii studentov "Sibirskie yuridicheskie studencheskie chteniya"* [Proc. 18th Int. Conf. "Siberian law student readings"]. Omsk, pp. 204-207.
3. Kryukova I.V., Alimamedov E.N. (2021) Fishing kak vid internet-moshennichestva [Phishing as a type of Internet fraud]. *Naukosfera* [Scientific sphere], 2-2, pp. 196-201.
4. Mal'chenkova V.V., Mal'chenkov E.V., Sologubov A.Yu. (2021) Moshennichestvo kak sotsial'no-pravovoe yavlenie [Fraud as a social and legal phenomenon]. *Aktual'nye problemy bor'by s prestupleniyami i inymi pravonarusheniyami* [Topical problems of combating crimes and other offenses], 21-2, pp. 24-26.
5. *O gosudarstvennom regulirovanii deyatel'nosti po organizatsii i provedeniyu azartnykh igr i o vnesenii izmenenii v nekotorye zakonodatel'nye akty Rossiiskoi Federatsii: feder. zakon Ros. Federatsii ot 29.12.2006 № 244-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 20.12.2006: odobr. Sovetom Federatsii Feder. Sobr. Ros. Federatsii 27.12.2006* [On the state regulation of activities related to the organization and conduct of gambling and on amending certain legislative acts of the Russian Federation: Federal Law of the Russian Federation No. 244-FZ of December 29, 2006]. Available at: http://www.consultant.ru/document/cons_doc_LAW_64924/ [Accessed 04/03/21].
6. Potapova A.V. (2020) Moshennichestvo v seti internet: kriminologicheskaya kharakteristika i problemy kvalifikatsii [Fraud on the Internet: criminological characteristics and the problems of legal assessment]. *StudNet*, 3 (6), pp. 52-57.
7. Sergeev D.R., Lyubimenko O.A., Savvateeva O.V. (2020) Moshennichestvo v seti internet kak ugroza ekonomicheskoi bezopasnosti gosudarstva [Fraud on the Internet as a threat to the economic security of the state]. *Teoreticheskaya ekonomika* [Theoretical economics], 3, pp. 76-84.
8. *Ugolovnoe pravo v ponyatiyakh i terminakh* [Criminal law in concepts and terms] (2019). Saransk.
9. *Ugolovnyi kodeks Rossiiskoi Federatsii: feder. zakon Ros. Federatsii ot 13.06.1996 № 63-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 24.05.1996: odobr. Sovetom Federatsii Feder. Sobr. Ros. Federatsii 05.06.1996* [Criminal Code of the Russian Federation: Federal Law of the Russian Federation No. 63-FZ of June 13, 1996]. Available at: http://www.consultant.ru/document/cons_doc_LAW_10699/ [Accessed 04/03/21].
10. *V Permi vynesen prigovor vinovnomu v serii prestuplenii v sfere telekommunikatsii i komp'yuternoi informatsii* [In Perm, a sentence was passed to a person guilty of a series of crimes in the field of telecommunications and computer information]. Available at: https://59.xn--b1aew.xn--p1ai/news/item/15783318 [Accessed 04/03/21].
11. *V Tyumeni budut sudit' zhitelya Permi za khishchenie 10,5 mln rublei s pomoshch'yu virusnogo PO* [In Tyumen, a resident of Perm will be tried for stealing 10.5 million rubles with the help of virusware]. Available at: https://www.kommersant.ru/doc/4637386 [Accessed 04/03/21].