УДК 34 DOI: 10.34670/AR.2020.23.36.021

Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ): понятие, уголовно-правовая характеристика и некоторые особенности расследования

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

Асанова Ирина Павловна

Кандидат филологических наук,
доцент кафедры уголовного права и криминологии,
Саранский кооперативный институт (филиал),
Российский университет кооперации,
430027, Российская Федерация, Саранск, ул. Транспортная, 17;
E- mail: i.p.asanova@rucoop.ru

Данилов Вадим Владимирович

Кандидат юридических наук,
доцент кафедры уголовного процесса и криминалистики,
Саранский кооперативный институт (филиал),
Российский университет кооперации,
430027, Российская Федерация, Саранск, ул. Транспортная, 17;
E- mail: vdanilov@ruc.su

Аннотация

Проводимые в конце XX – начале XXI века экономико-правовые и социально-политические преобразования активизировали научный поиск модели достижения эффективного развития российской государственности, ее экономики. В этих условиях развитие общества невозможно без формирования правовой базы, которая эффективно обеспечила бы экономическую безопасность государства. Государство, выступая гарантом стабильности отношений собственности на основе Конституции Российской Федерации, обеспечивает устойчивое их развитие. Конституция как основной закон декларирует равенство всех форм собственности, равную их защиту.

В данной статье авторами рассматриваются и анализируются особенности специального вида мошенничества, закрепленного в ст. 159.6 УК РФ; особенности состава данного преступления. Особое внимание уделяется рассмотрению современных способов

совершения мошенничества в сфере компьютерной информации.

Для цитирования в научных исследованиях

Абдульмянова Т.В., Асанова И.П., Данилов В.В. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ): понятие, уголовно-правовая характеристика и некоторые особенности расследования // Вопросы российского и международного права. 2021. Том 11. № 1А. С. 134-145. DOI: 10.34670/AR.2020.23.36.021

Ключевые слова

Уголовное право, уголовный закон, экономическая безопасность, противодействие экономической преступности, криминализация имущественных отношений, защита собственности, уголовно-правовые методы защиты, виды мошенничества, состав мошенничества, специальный состав мошенничества, способы совершения интернет-мошенничества, уголовная ответственность, уголовное наказание, санкции.

Введение

Исследование проблем противодействия экономической преступности показывает, что соответствующие правовые институты функционируют неэффективно, создают серьезные препятствия на пути дальнейшего улучшения благополучия общества. Наблюдается системное запаздывание со стороны законодателя с адекватной правовой оценкой динамики имущественных отношений. В отдельных случаях законодательные новеллы принимаются без социально-экономической обоснованности и достаточной научной проработанности, законодатель не учитывает реальную обстановку, руководствуется интересами отдельных групп лиц. Повышение эффективности правового регулирования института имущественных отношений, таким образом, является серьезной проблемой для законодателя.

Криминализация имущественных отношений, оказывая негативное влияние на экономику, принуждает законодателя расширить сферу уголовно-правового воздействия. В этих условиях и с учетом массового характера проявления злоупотреблений в сфере имущественных отношений возникла острая необходимость обобщения национального, зарубежного опыта законодательной регламентации ответственности за преступления против собственности.

Очевидной является необходимость проведения критического исследования и оценки многих законодательных положений о преступлениях против собственности. Безусловно, нужна объективная оценка криминальных последствий, потребуется разработка инновационных по содержанию уголовно-правовых мер защиты собственности. Необходимо и обобщение судебно-следственной практики применения норм Уголовного кодекса Российской Федерации (УК РФ) о преступлениях в сфере имущественных отношений. В ней возникает ряд проблем, связанных с квалификацией преступлений, отграничением их друг от друга. Представляется, что изложенное убедительно подтверждает актуальность, теоретическую и практическую ценность монографического исследования, которое осуществлено автором на стыке теории уголовного права, криминологии и других наук на основе комплексного исследования теоретических и методологических проблем законодательной регламентации уголовной ответственности за преступления против собственности. Изучение результатов научных изысканий по рассматриваемой проблеме показало, что в них высказываются различные суждения по уголовно-правовой оценке преступлений против собственности, феномена «хищение», признаков преступлений, их систематизации, взаимосвязи и

взаимозависимости уголовно-правовых норм, что указывает на недостаточную научную разработанность данного научного направления. Отечественные ученые внесли существенный вклад в разработку и применение уголовно-правовых норм об ответственности за хищение чужого имущества. Фундаментальную основу доктрины уголовного права и криминологии по рассматриваемым проблемам сформировали такие ученые, как А.И. Алексеев, Д.И. Аминов, В.К. Бабаев, В.М. Баранов, А.Г. Безверхов, Ю.В. Блувштейн, В.Н. Бурлаков, А.А. Витвицкий, В.А. Владимиров, Б.В. Волженкин, А.В. Галахова, И.М. Гальперин, Л.Д. Гаухман, А.А. Герцензон, Я.И. Гилинский, А.А. Глухова, С.П. Голубятников, С.А. Гордейчик, Г.Н Горшенков, П.С. Дагель, А.В. Данилов, А.И. Долгова, А.Э. Жалинский, В.Н. Зырьянов, С.А. Елисеев, М.Г. Иванов, И.И. Карпец, А.К. Квициния, И.Я. Козаченко, А.А. Конев, С.М. Кочои, Л.Л. Кругликов, В.Н. Кудрявцев, А.П. Кузнецов, Н.Ф. Кузнецова, Н.А. Лопашенко, Ю.И. Ляпунов, М.В. Максимов, А.Г. Маркушин, В.Е. Мельникова, М.Г. Миненок, П.Н. Панченко, А.А. Пионтковский, М.В. Степанов, В.Я. Таций, Э.С. Тенчов, А.Н. Трайнин, В.И. Тюнин, С.И. Улезько, В.С. Устинов, А.Я. Фойницкий, Е.Е. Черных, А.Ю. Чупрова, А.В. Шульга, А.М. Яковлев, П.С. Яни и др.

Вместе с тем следует отметить, что достаточно сложная и многоаспектная проблема противодействия преступлениям в сфере имущественных отношений до настоящего времени не разрешена. Отдельные вопросы не разработаны в достаточной степени в теории, ряд вопросов продолжают оставаться спорными или получили неоднозначное толкование, некоторые не нашли своего отражения в законодательстве. Важно обратить внимание на то, что большинство исследований проводилось по отдельным направлениям криминологии или уголовного права, а изучение законодательной регламентации уголовной ответственности за хищение и проблем формирования законодательства в целом не носило комплексного характера. Кроме того, многие научно-теоретические исследования проводились до принятия УК РФ 1996 года, внесения в него последующих изменений. Более того, не уменьшающийся массив хищений чужого имущества побуждает к разработке новых, более эффективных мер воздействия.

В этих условиях назрела необходимость проведения комплексного научно-прикладного исследования законодательной регламентации уголовной ответственности за совершение преступлений против собственности, которая диктуется как потребностями практики, так и задачами дальнейшего совершенствования теории, законодательной и правоприменительной практики в контексте глобальных изменений социально-экономической жизни в современной России. Внимание и усилия автора обращены как на дальнейшее развитие основ теории уголовного права о преступлениях в сфере имущественных отношений, так и на разработку новых норм и внесение изменений, корректив в ныне действующее уголовное законодательство на основе глубокого анализа как национальной законодательной, следственной и судебной практики, так и зарубежных стран.

Обоснованность введения нормы ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации»

Современный этап общественного развития связан с повсеместным проникновением и использованием сети Интернет. Однако вместе с явными преимуществами, такими, как мгновенный доступ к информации, возможность онлайн оплаты товаров и практически любых видов услуг, условия для мгновенной и беспрепятственной коммуникации с любой точкой мира, развитие сети Интернет несет и глобальные угрозы, снижающие экономическую безопасность государства. Одной из таких угроз, является Интернет-мошенничество, которое развивается

вместе с глобальной сетью [Иващенко Н.Д., 2020, С. 269-276].

Следует заметить, что стремительное развитие сети Интернет во втором десятилетии 21 века приводит к тому, что развитые государства постепенно осуществляют переход от традиционной к информационной (цифровой) экономике.

Это касается и Российской Федерации, где 24 декабря 2018 года решением президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам утвержден паспорт национальной программы «Цифровая экономика Российской Федерации».

Однако стоит понимать, что переход к цифровым экономикам, и, как следствие, глобализация национальных экономик в единую глобальную систему, а также взаимная интеграция оказывают не только положительное влияние на социально-экономическое развитие государства, но и несут в себе ряд серьезных угроз его экономической безопасности. Одним из факторов, неблагополучно влияющих на состояние национальной экономики, является развитие преступности и мошеннической деятельности, которая в условиях глобального распространения сети «Интернет» видоизменяется и интегрируется в сферы Интернет-торговли, Интернет-маркетинга и прочих товарно-денежных отношений в глобальной сети, подрывая постулаты экономической безопасности государства.

Как известно, подрыв экономической безопасности приводит к ослаблению национальной безопасности государства [Калинин Д.Д., 2015, С. 15-16]. Поэтому в современных реалиях развитие преступности и мошенничества в сети Интернет следует рассматривать как одну из крупнейших угроз национальной безопасности и изыскивать действенный инструментарий противодействия, отвечающий требованиям времени и актуализирующийся в процессе происходящих изменений.

Рассмотрение компьютерного мошенничества основывается на результатах исследований зарубежных и российских ученых-экономистов и юристов, занимающихся изучением вопросов нивелирования проблем, порождаемых преступностью и мошеннической деятельностью, и актуальных методов обеспечения экономической безопасности государства: Калинина Д.Д., Балога М.М., Богомолова В.А., Орлова И.А., Сенчагова В.К. и др [Сергеев Д.Р., 2020, С. 76-84].

Так, Сенчагов В.К. в своих работах основывается на институциональном определении экономической безопасности, делая акцент на властных структурах, которые должны обеспечивать национальную безопасность страны путем выработки правильного социально-экономического развития, умелого управления оборонным комплексом, представления и защиты национальных интересов, а также выявления потенциальных экономических угроз [Сенчагов В.К., 2015, С. 237-238].

Не менее важное значение имеют исследования информационных технологий и механизмов цифровизации экономических отношений, отраженные в работах таких авторов, как Хачатурян М.В., Андреас М.А., Корольков В.Е., Ерофеева Т.А., Карпунина Е.К. и др.

Попытки изучения влияния Интернет-преступности и мошенничества на состояние экономической безопасности государства предпринимали такие авторы, как Никитина И.А., Демидова А.С., Поляруш А.А., Толкачева А.П. и многие др. Однако, несмотря на проводимые исследования угроз экономической безопасности, связанных с возрастанием цифрового мошенничества, на данный момент отсутствует комплексный инструментарий нивелирования подобных угроз, что актуализирует необходимость его разработки и последующей корректировки [Ефимова Э.Н., 2020, С. 55-58].

Согласно открытой статистике министерства внутренних дел России, с января по сентябрь

2019 года было совершено более 205000 преступлений с использованием информационно-телекоммуникационных технологий, что в процентном соотношении больше на 69%, чем в соответствующем предыдущем периоде. Если брать во внимание отчетность предыдущих лет, то, по состоянию отчетного периода с января по сентябрь 2018 года, было официально зарегистрировано 121247 преступлений аналогичного характера. В целом прослеживается тенденция устойчивого роста данного типа правонарушений: в период с 2017-2019 гг. количество преступлений, совершенных с использованием информационных технологий выросло более чем в три раза.

Соответственно растет и размер причинённого ущерба. Согласно оценкам экспертов МВД, ежегодно только в российском сегменте сети Интернет мошенники совершают противоправные действия на суммы около 450 миллионов долларов, а ущерб от подобных действий приводит к подрыву экономической безопасности государства.

Тенденций к уменьшению темпов роста правонарушений и мошеннический деяний в сети Интернет в ближайшей перспективе не предвидится в силу того, что он прямо пропорционален росту пользователей глобальной сети. Все больше людей вовлекаются во взаимодействие посредством использования сети Интернет, совершенствуются средства связи, и большая часть населения активно обменивается информацией с помощью разнообразных приложений [Ерофеева Т.А., 2019, С. 16-17]. Темпы развития беспроводных и проводных способов передачи данных также увеличиваются, в ближайшие годы интернетификация будет охватывать даже самые отдаленные регионы [Карпунина Е.К., 2019, С. 28-41]. Данная тенденция усиливается под влиянием роста объемов финансирования, выделяемых на развитие сетей подобного типа в соответствии с задачами Правительства России и Министерства связи и массовых коммуникаций [Сайт правительства Российской Федерации…URL].

Приведенные факты обращают исследовательское внимание на существование условий для устойчивого роста количества преступлений и мошеннических операций в информационной сфере и расширение способов и форм данных противоправных деяний.

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 [Абдульмянова Т.В., 2018, С. 140].

Федеральным законом РФ «О внесений изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 29 ноября 2012 г. № 207 – ФЗ Уголовный кодекс 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 в понятиях…2019, С. 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 приобретения 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), а равно приобретения им юридического права на распоряжение такими деньгами (имуществом).

Субъективную сторону мошенничества в сфере компьютерной информации образует прямой умысел на завладение чужим имуществом посредством незаконного вторжения в функционирование средств компьютерной информации.

Субъектом преступления признается физическое вменяемое лицо, достигшее 16 лет.

Классификация современных способов Интернет-мошенничества

Далее 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 С.А., 2020, С. 3-9]:

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 по стопроцентной предоплате. Соответственно, жертва, осуществив перевод денежных средств, не получает требуемого товара. 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 слабозащищённых и не осведомленных граждан с учетом низкого уровня их информационной грамотности.

2) Фишинг – является чуть более продвинутым видом Интернет-мошенничества. Целью мошенника в таком случае становится возможность завладеть банковскими реквизитами, данными электронных платежных карт либо данными от электронных Интернет-кошельков пользователей. Фишинговый сайт сложно распознать ввиду того, что он полностью копирует оригинальный сайт, например, может быть полностью скопирован интерфейс какого-либо клиент-банка (в основном, актуально для физических лиц, так как клиент-банки у юридических лиц защищены средствами крипто шифрования и усиленных цифровых подписей), отличие будет составлять лишь адрес доменного имени, не привлекающий внимание неподготовленного гражданина. В такой ситуации жертва добровольно вводит свои учетные данные от кошелька либо банковской карты и в скором времени теряет денежные средства с данного носителя.

3) Черный инфобизнес – популярный вид Интернет-мошенничества, начиная с конца 2017 года. Стоит отметить, что сам по себе инфобизнес не является мошенничеством, поскольку представляет собой продажу информации в форме книг, аудио и видео файлов, 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 ментерство 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.

4) Мошенничество с распространением контента – представляет собой вид мошенничества, при котором мошенниками создается архив с требуемой пользователю информацией. Как правило, срабатывает несложный скрипт, подменяющий название архива на запрашиваемую пользователем информацию в поисковой системе. Но 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.

5) Финансовые пирамиды, которые законодательно запрещены на территории Российской Федерации, независимо от того, является ли она традиционной финансовой пирамидой либо Интернет-проектом. Несмотря на то, что за организацию финансовых пирамид установлена уголовная ответственность, финансовые пирамиды 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 партнёров, имеющих аналогичные права. При этом доход каждого участника сети состоит из комиссионных за реализацию продукции и дополнительных вознаграждений (бонусов), зависящих от объёма продаж, совершённых привлечёнными 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.

6) 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 пунктом 3 Федерального закона от 29.12.2006 № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации», 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. Организация и (или) проведение азартных игр с использованием игрового оборудования вне игорной зоны либо с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», а также средств связи, в том числе подвижной связи, – влекут наложение административного штрафа на граждан в размере от трех

тысяч до пяти тысяч рублей с конфискацией игрового оборудования; на должностных лиц – от тридцати тысяч до пятидесяти тысяч рублей с конфискацией игрового оборудования; на юридических лиц – от семисот тысяч до одного миллиона рублей с конфискацией игрового оборудования. Проблема регулирования казино в сети Интернет состоит в том, что в 90% случаев компании, владеющие данными ресурсами, являются зарегистрированными 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.

Можно сказать о том, что как правовое, так и техническое регулирование противоправных действий в телекоммуникационных сетях попадает в безвыходную ситуацию.

Выходом из сложившейся ситуации может 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 А.В., 2020, С. 52-57].

Заключение

Регуляторами и гарантами соблюдения прав и свобод пользователей сети Интернет на территории Российской федерации сегодня выступают Министерство внутренних дел, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Федеральная антимонопольная служба, Федеральная налоговая служба, действующие согласно действующему на сегодняшний день законодательству.

Учитывая данные о количестве обращений граждан, подвергшихся противоправным действиям в сети Интернет, растущей технической и юридической грамотности преступников, можно прийти к неутешительному выводу, что данных мер противодействия мошенничеству в сети Интернет недостаточно.

Следует отметить, что на территории Российской Федерации, начиная с 2011 года с целью противодействия преступным деяниям в сети Интернет и защиты физического и нравственного здоровья граждан, были созданы общественные организации «Кибердружина», «Киберпатруль», «Медиагвардия» и другие [Брайко Д. Н., 2017, С. 24-25]. Однако деятельность подобных организаций на текущий момент до конца не регламентирована законодательно, а уровень технической подготовки волонтеров, состоящих в данных организациях, оказывается не всегда высоким.

Укрепление 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 посредством взаимодействия Совета по обеспечению

экономической безопасности с высококвалифицированными специалистами технических областей. Для реализации данной меры необходимо создание технически оснащенного и наполненного квалифицированными кадрами отделения при Совете безопасности Российской Федерации, к функционалу которого будет относиться формирование базы нелегальных сайтов и ведение координационной работы со специалистами технической поддержки интернет-провайдеров, хостингов и ведущих мировых социальных сетей с целью максимально оперативного блокирования сайтов и аккаунтов мошеннических организаций. Рабочий состав подобного аппарата должен состоять из взаимодействующих друг с другом специалистов юридической направленности, специалистов технических областей, специалистов экономической безопасности, итогом деятельности которых будет информационно-аналитическое обеспечение предупреждения, выявления, пресечения, раскрытия и расследования экономических и налоговых преступлений, связанных с противоправными действиями в сети Интернет. Опираясь на возможности современного информационно-технологического развития, в частности, доступ к использованию инструментов машинного обучения, при работе с огромными массивами данных, группе специалистов потребуется помощь самообучающихся нейронных сетей, самостоятельно принимающих решение о противоправной направленности того или иного Интернет-ресурса.

Учитывая, что 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 и их зеркал без решения суда. Судебные разбирательства могут пролонгироваться 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.

Таким образом, актуальной задачей становится создание многоуровневой, протестированной системы взаимодействия исключительно опытных и высококлассных специалистов с использованием алгоритмов самообучающихся нейронных сетей. Как только информация с нежелательного сайта будет проанализирована группой специалистов и будет вынесен вердикт о блокировке, информация с данного сайта должна быть помещена в базу данных нейросети, которая, используя алгоритмы поисковых систем и вычислительные мощности серверов, находящихся в подчинении аппарата контроля за противоправной информацией в сети Интернет, будет самостоятельно идентифицировать клоны данного сайта и принимать решение об их блокировке.

В результате проведенного исследования можно сделать вывод, что решение проблем, связанных с мошеннической деятельностью в сети Интернет, должно быть одним из первостепенных и безотлагательных вопросов на повестке современного аппарата управления государством. Требуется не только совершенствование и модернизация современного

законодательства, регулирующего деятельность в глобальной 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 сети. Требуется выстроить полноценное взаимодействие специалистов в области юриспруденции, управления и технологического обеспечения, путем формирования площадок для их совместной работы.

Библиография

1. Абдульмянова Т.В., Фролкина И.А. Предупреждение мошенничества в сфере материнского капитала // Вопросы российского и международного права. 2018. № 10. С. 139-144.
2. Борсученко С.А., Амосов Е.А. Мошенничество в сфере компьютерной информации: вопросы теории и практики // В сборнике: Цифровизация рыночных отношений: вопросы экономики и права 2020. С. 3-9.
3. Брайко Д. Н. Опыт организации добровольного молодежного движения: от «Кибердружины» к «Интернету без угроз» // Обзор НЦПТИ. 2017. №2 (11). С. 24-25.
4. Ерофеева Т.А. Цифровая трансформация экономики в условиях геоэкономической нестабильности. М., 2019. С. 16-17.
5. Ефимова Э.Н. Мошенничество в условиях цифровизации экономики. меры профилактики и пресечения // Студенческий вестник. 2020. № 23-2 (121). С. 55-58.
6. Иващенко Н.Д. Мошенничество в сфере компьютерной информации: проблемные вопросы // Столица науки. 2020. № 6 (23). С. 269-276.
7. Калинин Д.Д. Экономическая безопасность России. М., 2015. С. 15-16.
8. Карпунина Е. К., Горчев Й. Цифровые изменения экономической системы: от стратегии догоняющего развития к институтам опережения // Друкеровский вестник. 2019. №3. С. 28-41.
9. Потапова А.В. Мошенничество в сети интернет: криминологическая характеристика и проблемы квалификации // StudNet. 2020. Т. 3. № 6. С. 52-57.
10. Сайт правительства Российской Федерации // URL.: http://www.goverment.ru (дата обращения: 11.11.2020).
11. Сенчагов В.К. Экономическая безопасность России. М., 2015. С. 237-238.
12. Сергеев Д.Р., Любименко О.А., Савватеева О.В. Мошенничество в сети интернет как угроза экономической безопасности государства // Теоретическая экономика. 2020. № 3 (63). С. 76-84.
13. Уголовное право в понятиях и терминах [Текст]: учеб. пособие / [авт.-сост.: Т.В. Абдульмянова, И.П. Асанова, С.Б. Котляров] ; Саран. кооп. ин-т (фил.) РУК. Саранск: Редакционно-издательский центр МГПИ, 2019. 80 с.

Fraud in the field of computer information (article 159.6 of the Criminal Code of the Russian Federation): concept, criminal law characteristics and some features of the investigation

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

Irina P. Asanova

PhD in Philology, 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: i.p.asanova@rucoop.ru

Vadim V. Danilov

PhD in Law
Associate Professor of the Department
of Criminal Procedure and Forensic Science,
Saransk Cooperative Institute (branch),
Russian University of Cooperation,
430027, 17 Transportnaya st., Saransk, Russian Federation;
e- mail: vdanilov@ruc.su

Abstract

The economic, legal and socio-political transformations carried out in the late XX – early XXI centuries have intensified the scientific search for a model for achieving effective development of the Russian statehood and its economy. In these conditions, the development of society is impossible without the formation of a legal framework that would effectively ensure the economic security of the state. The state, acting as the guarantor of the stability of property relations on the basis of the Constitution of the Russian Federation, ensures their sustainable development. The Constitution as the basic law declares the equality of all forms of property, their equal protection.

In this article, the authors examine and analyze the features of a special type of fraud, enshrined in Art. 159.6 of the Criminal Code of the Russian Federation; features of the composition of this crime. Particular attention is paid to the consideration of modern methods of committing fraud in the field of computer information.

For citation

Abdul'myanova T.V., Asanova I.P., Danilov V.V. (2021) Moshennichestvo v sfere komp'yuternoi informatsii (st. 159.6 UK RF): ponyatie, ugolovno-pravovaya kharakteristika i nekotorye osobennosti rassledovaniya [Fraud in the field of computer information (article 159.6 of the Criminal Code of the Russian Federation): concept, criminal law characteristics and some features of the investigation]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 11 (1A), pp. 134-145. DOI: 10.34670/AR.2020.23.36.021

Keywords

Criminal law, criminal law, economic security, combating economic crime, criminalization of property relations, protection of property, criminal legal methods of protection, types of fraud, composition of fraud, special composition of fraud, methods of committing Internet fraud, criminal liability, criminal punishment, sanctions.

References

1. Abdul'myanova T.V., Frolkina I.A. Fraud prevention in the sphere of maternity capital // Issues of Russian and international law. 2018. No. 10. P. 139-144.
2. Borsuchenko S.A., Amosov E.A. Fraud in the field of computer information: issues of theory and practice // In the collection: Digitalization of market relations: issues of economics and law. 2020. P. 3-9.
3. Braiko DN Experience of organizing voluntary youth movement: from «Cyberdruzhina» to «Internet without threats» // Review of NTSPTI. 2017. No. 2 (11). S. 24-25.
4. Erofeeva T.A. Digital transformation of the economy in the context of geoeconomic instability. M., 2019. S. 16-17.
5. Efimova E.N. Fraud in the context of the digitalization of the economy. measures of prevention and suppression // Student Bulletin. 2020. No. 23-2 (121). S. 55-58.

6. Ivaschenko N.D. Fraud in the field of computer information: problematic issues // Capital of Science. 2020. No. 6 (23). S. 269-276.
7. Kalinin D.D. Economic security of Russia. M., 2015. S. 15-16.
8. Karpunina EK, Gorchev Y. Digital changes in the economic system: from the strategy of catch-up development to the institutions of anticipation // Drucker's bulletin. 2019. No. 3. S. 28-41.
9. Potapova A.V. Fraud on the Internet: criminological characteristics and qualification problems // StudNet. 2020.Vol. 3. No. 6. P. 52-57.
10. The website of the government of the Russian Federation // URL.: http://www.goverment.ru (date of access: 11.11.2020).
11. Senchagov V.K. Economic security of Russia. M., 2015. S. 237-238.
12. Sergeev D.R., Lyubimenko O.A., Savvateeva O.V. Fraud on the Internet as a Threat to the Economic Security of the State // Theoretical Economics. 2020. No. 3 (63). S. 76-84.
13. Criminal law in concepts and terms [Text]: textbook. manual / [author-comp.: T.V. Abdulmyanova, I.P. Asanova, S.B. Kotlyarov]; Saran. co-op. Institute (Phil.) RUK. Saransk: Editorial and Publishing Center of Moscow State Pedagogical Institute, 2019. 80 p.