УДК 343 **Юридические науки**

Лубяная Наталья Игоревна, *студентка 2-го курса кафедры «Цифровая криминалистика», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация*

СОВРЕМЕННЫЙ ВЗГЛЯД НА ВИДЫ ПРЕСТУПЛЕНИЙ В СФЕРЕ IT-ТЕХНОЛОГИЙ: СПОРНЫЕ ВОПРОСЫ И ИХ РЕШЕНИЯ

Аннотация: В статье рассмотрены особенности квалификации преступлений с использованием информационных технологий, связанные с неправомерным доступом к компьютерной информации, созданием и распространением вредоносных программ, финансовым мошенничеством, совершаемым посредством методов социальной инженерии, а также кибермошенничеством. Проанализирована актуальность этих составов в контексте мировой пандемии COVID-19 и связанных с ней ограничений на основании статистики правоохранительных органов и аналитических данных компаний Positive Technologies и Group-IB, занимающихся вопросами информационной безопасности. Предложены решения проблем квалификации преступлений с учётом новелл уголовного права на момент проведения исследования и анализа особенностей правоприменительной практики и современных тенденций киберпреступности.

Ключевые слова: IT-преступность, социальная инженерия, онлайн-сервисы, персональные информационные ресурсы, финансовые ресурсы, кибермошенничество, киберугроза

Abstract: The article deals with the features of qualification of crimes using information technologies related to illegal access to computer information, creation and distribution of malicious programs, financial fraud committed through social engineering methods, as well as cyber fraud. The relevance of these formulations in

the context of the global COVID-19 pandemic and related restrictions is analyzed on the basis of law enforcement statistics and analytical data from Positive Technologies and Group-IB companies dealing with information security issues. Solutions to the problems of crime qualification are proposed, taking into account the novelties of criminal law at the time of research and analysis of the features of law enforcement practice and current trends in cybercrime.

Keywords: IT crime, social engineering, online services, personal information resources, financial resources, cyber fraud, cyber threat

Введение

В условиях активного мирового информационно-технологического прогресса важным фактором является обеспечение безопасности в этой сфере. Однако наиболее остро этот вопрос встает перед обществом во время масштабного общего спада. Как и любое масштабное кризисное явление пандемия COVID-19 (весна - осень 2020 года) дестабилизировала не только мировую и национальные экономики, но и жизнь общества в целом, в том числе повлияла на рост киберугрозы в связи с вынужденной цифровизацией и складыванием благоприятной среды для активизации деятельности соответствующего преступного сегмента. В связи с этим обеспечение информационной безопасности российского общества стало ещё более актуальным. Согласно статистике Генеральной Прокуратуры и МВД России в 2019 году рост IT- преступности составил 68% по сравнению с 2018 г. –15 % от общего количества преступлений, а в 2020 году только за первые 7 месяцев преступность с использованием IT-технологий выросла на 91, 7 % по сравнению с аналогичным периодом прошлого года, составив 23% от общего количества преступлений [11; 15].

Рис.1 Статистика IT- преступлений [11]

Наиболее пострадавшими от IT-преступлености правоохранительные органы [10] и ИБ-компании (компании, занимающиеся информационной безопасностью) [1] в отчетах о своей деятельности называют банковский и бизнес сегменты, а также персональные информационные ресурсы пользователей. Подобная динамика объясняется тем, что в период действия карантинных мер практически все сферы жизни общества были переведены в виртуальную среду. С переходом большей части компаний на дистанционную работу, многократно увеличился риск посягательства на их конфиденциальную информацию, включающую объекты исключительных прав (ноу-хау, патентоохраняемые объекты, иную коммерческую информацию) и финансовую сферу как со стороны конкурентов, так и со стороны преступных элементов, преследующих корыстные мотивы. Сфера персональной информации пользователей компьютеров, смартфонов и других современных устройств в условиях пандемии и связанных с ней карантинных мер, представляется потенциально наиболее уязвимой для киберпреступников, поскольку большая часть людей не обладает специальными знаниями в области защиты информации, а многие из них пренебрегают системами защиты информации, предлагаемыми на рынке соответствующих услуг. В условиях самоизоляции и

дистанционной работы активно стали использоваться электронные финансовые инструменты (онлайн-переводы, электронные кошельки и т.д.) для оплаты товаров и услуг, проведения транзакций по закупкам между компаниями, также ставшие основными объектами посягательства киберпреступников на банковскую сферу.

Таким образом, связи с возросшей киберугрозой стали наиболее актуальными составы преступлений, связанные с кибермошенничеством, неправомерным доступом к компьютерной информации, созданием и распространением вредоносных компьютерных программ, рассмотрение особенностей которых в контексте современной обстановки требует детального изучения в контексте данного исследования.

Средства и способы неправомерного доступа к компьютерной информации, создание и распространение вредоносных компьютерных программ, мошенничество и связанные с ними особенности квалификации преступлений.

Как было отмечено ранее, вынужденный, в условиях самоизоляции, переход населения России в цифровую сферу взаимодействия, сделал необходимым для каждого использование сети Интернет, посредством которой в этот период (весна-осень 2020 года) происходило обеспечение как потребностей отдельных граждан в получении образования, совершении покупок, оплате услуг, общении, обеспечении досуга, так и интересов всех отраслей крупного, среднего и малого бизнеса в обеспечении деятельности компаний посредством организации взаимодействия их структурных элементов с использованием корпоративных средств связи (электронные почты, мессенджеры и т.д.) и дистанционной торговли с помощью электронных финансовых инструментов. Такая трансформация общественной жизни стала благоприятной средой для повышения угрозы информационной безопасности и роста киберпреступности, поскольку пользователи компьютеров, смартфонов и иных устройств достаточно часто не обеспечивают собственную

информационную безопасность в силу недостатка компьютерной грамотности, а информационная безопасность некоторых компаний находится на низком уровне из-за малоинформированности сотрудников о способах её обеспечения, экономии на лицензионном программном обеспечении и антивирусном программном обеспечении, быстроизменяющихся условий и вынужденного перехода в дистанционный формат работы. В то же время преступный сегмент, обладая специальными знаниями о степени уязвимости различных информационных ресурсов, может использовать их в своих целях. Согласно отчетам о состоянии преступности Генеральной Прокуратуры [11] и МВД [10] от 2020 года наиболее распространенным мотивом совершения рассматриваемых преступлений в период пандемии является корысть [6], то есть стремление получить материальную выгоду от совершения определенных действий, а согласно исследованиям, проведенным Group-IB [1] и Positive Technologies [2] наиболее популярными объектами посягательства среди киберпреступников являются онлайн-сервисы, персональные и финансовые информационные ресурсы.

На первом месте по статистическим данным Group-IB и Positive Technologies находится посягательство на онлайн-сервисы [1]. Это обусловлено тем, что именно они чаще всего пользуются спросом у пользователей сети Интернет, обеспечивая удовлетворение многих потребностей, и концентрируют большой финансовый оборот в сети. Доставка товаров, просмотр фильмов, прослушивание музыки и другие услуги осуществлялись во время карантина и осуществляются в настоящее время посредством онлайн-серверов. Этим обстоятельством воспользовались преступники, причем не только в целях хищения денежных средств, но и для распространения недостоверной информации среди пользователей и наведения паники в обществе относительно реальной обстановки с COVID-19. Генеральный директор ВОЗ д-р Тедрос Гебрейесус, обращаясь к участникам Конференции по безопасности, проходившей в середине февраля в Мюнхене заявил, что «Бороться приходится не только с

эпидемией COVID-19, но и с “инфодемией” — распространением недостоверной информации» [8]. Проиллюстрировать «инфодемию» в России можно на примере недостоверных сообщений, о неправдоподобной статистике распространения коронавируса, возможности его лечения народными средствами и т.д., которые активно заполняют сеть с самого начала пандемии. В связи с этим в Уголовный кодекс РФ 1 апреля 2020 года была введена новая норма – ст. 207.1, предусматривающая наказание за публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан. В контексте преступлений с использованием IT- технологий важным представляется способ реализации деяния, предусмотренного ст. 207.1 УК РФ - использование сетевых ресурсов [13]. По данной статье весной 2020 года уже был вынесен первый приговор суда, по которому Екатерине Храпченковой было назначено наказание в виде 120 часов обязательных работ за публичное распространение ложной информации в веб-сервисе для публичного обмена видеоматериалами («Тик-Ток») ложной информации посредством видеоролика с комментарием о том, что приобретенная ей упаковка защитных масок является реализуемой за плату гуманитарной помощью [11]. Если при этом с целью размещения недостоверной информации был осуществлен неправомерный доступ к онлайн-сервису с использованием вредоносного ПО, то необходимо будет дополнить квалификацию деяния преступника положениями статей 272 и (или) 273 УК РФ. В случаях, когда хищение денежных средств сопряжено с неправомерным доступом к электронным платежным инструментам пользователей онлайн-сервисов, преступники осуществляют свои деяния посредством либо усовершенствованных с учетом развития технологий программ-шифровальщиков или криптолокеров- вредоносных программ, которые при активизации осуществляют блокирование существующей персональной информации пользователя в зависимости от прописанного в ней алгоритма, предоставляя преступникам возможность использовать полученную информацию по своему усмотрению, либо посредством фишинговых ссылок,

переход по которым также может лишить пользователя информации, которой преступник воспользуется для совершения правонарушения (пароли, номера банковских карт и т.д.). Квалификация хищения денежных средств в зависимости от способов его осуществления может осуществляться по ст. 159 УК РФ, 159.6 УК РФ и (или) ст. 273 УК РФ, так как доступ к информации может осуществлялся посредством вредоносного ПО [13].

Следующей по количеству совершенных преступлений является группа персональных информационных ресурсов [1]. Она занимает второе место по количеству посягательств на нее. К персональным относятся ресурсы для обмена информацией и размещения личной информации. Из цели использования данного вида ресурсов следует, что изначально они предполагают использование их одним человеком или организацией. Электронная почта, в том числе корпоративная - это один из самых распространенных персональных информационных ресурсов Интернета, который подвергся атакам со стороны преступников во время действия карантинных мер. Для передачи сообщений пользователей используются собственные протоколы, для работы с которыми необходима программа-клиент (почтовый клиент). Унификация интерфейсов в сети Интернет привела к тому, что большинство сообщений получаются и отправляются конечному пользователю через Web-интерфейс с помощью браузеров. Информация, содержащаяся в почтовом ящике, является охраняемой законом. Это условие указывается в пользовательском соглашении. Таким образом, доступ к данной информации без ведома её хозяина является неправомерным. Рассмотрим в связи с этим возможные нарушения правил защиты персональной информации. Первое связано со сменой пароля почтового ящика третьим лицом (преступником), что приводит к блокированию доступа легального пользователя к информации [2]. Преступник будет привлечен к ответственности даже в том случае, если переписка не являлась целью преступления, так как данное деяние подпадает под понятие - блокирование информации. Второе нарушение связано с уничтожением переписки или её

части, которое, соответственно, приводит к утрате доступа к информации законного пользователя [2]. Возможность восстановления информации не влияет на квалификацию преступления. Третий вид нарушения связан с копированием переписки или её части: снимки с экрана, скриншоты, распечатки и т.д. [1]. Отметим также, что в случае с копированием информации коммерческих организаций, представляющей собой коммерческую тайну: ноу-хау, патентоохраняемые объекты и другая конфиденциальная информация, усложняется квалификация таких деяний. При назначении наказания будут применены не только статьи главы 28 УК РФ, но и ст. 146 УК РФ, а также нормы гражданского права, направленные на защиту объектов интеллектуальной собственности. По статистике копирование информации во время карантина занимало лидирующие позиции среди способов манипуляции с информацией. Наиболее активно в данном случае преступниками осуществлялось копирование продуктов авторских прав и реализация пиратских версий фильмов [1]. Последний вид нарушения в данной сфере связан с модификацией информации, например, рассылкой писем от имени жертвы, любым изменением настроек информации [1].

Актуальным с точки зрения киберпреступности персональными информационными ресурсами являются и социальные сети. Страница социальной сети содержит больший диапазон информации о потенциальной жертве (фотографии, ссылки, «репосты» и др.), переписка носит вторичный характер. Однако стоит отметить, что именно доступ к переписке можно назвать несанкционированным, информация на «стене», выложенная в публичном доступе, не является информацией, охраняемой законом от несанкционированного доступа. Единственное ограничение налагается на распространение информации, запрещённой законом. Таким образом, несанкционированным доступом к компьютерной информации будет только получение доступа к закрытой переписке или фото, -видео материалам. Особенность квалификации деяний при этом заключается в её зависимости от

объекта правонарушения. Таким образом, помимо статей главы 28 УК РФ [13], связанных с воздействием на компьютерную информацию, могут применяться ст. 146 УК РФ, при посягательстве на объекты интеллектуальной собственности, ст. 163 УК РФ, если компьютерная информация, добытая преступным путем используется с целью вымогательства денежных средств или иного имущества [3].

Группа финансовых ресурсов занимает третье место по количеству совершенных против неё преступлений [1]. К финансовым относятся средства, которые позволяют оперировать денежными средствами пользователя в любой форме и для любых целей. Высокая доля преступлений, связанных со счетами банковских карт, обусловлена возможностью управления таким счетом посредством мобильного телефона (SMS-банкинг). Уязвимость такой технологии обусловлена несколькими факторами. Во-первых, для осуществления транзакции не требуется банковская карта. Во-вторых, система идентификации пользователя не всегда отвечает всем требованиям безопасности [2]. Преступники достаточно часто пытались осуществить и попытки перевода денег с найденной банковской карты посредством онлайн-перевода, если к ней не была подключена двухуровневая система идентификации пользователя [9]. Для подтверждения онлайн-переводов преступники в настоящее время применяют методы социальной инженерии, получая доступ к банковским реквизитам, посредством убеждения потенциальной жертвы в том, что звонок осуществляется уполномоченным на то лицом (вишинг): сотрудником службы безопасности или отделения банка и т.д. Таким образом может быть получено подтверждение перевода денежных средств, пин-кодов, номеров банковских карт и т.д. В период пандемии коронавируса подобное хищение денежных средств осуществляется в том числе и посредством «двойного обмана жертвы», заключающегося в том, что людям, уже ставшим жертвами IT-преступников, мошенники под видом несуществующих организаций («Единый

центр возвратов, «Центра финансовой защиты») предлагают компенсировать нанесенный ущерб, однако вместо компенсации потерпевшие снова предоставляют преступникам идентификационные данные банковских карт и подвергаются хищению денежных средств [1]. Рассмотренные способы осуществления преступлений связаны прежде всего с манипулированием психологическим состоянием жертвы- применением методов социальной инженерии. Актуализация использования мошенниками подобных манипуляций, по мнению автора, связана прежде всего с вынужденным переводом на дистанционную работу банков и других финансовых организаций, что сделало необходимым для всех категорий потребителей банковских продуктов, в том числе потенциально уязвимых (пожилые люди, подростки и т.д.), использование дистанционных услуг, то есть произошло увеличение количества потенциальных жертв преступников. Существует определённая взаимосвязь и с общим психологическим состоянием людей в кризисный период, вызванный пандемией коронавируса, поскольку в связи с ростом безработицы, падением общего дохода населения, наиболее остро воспринимались непредвиденные финансовые потери, связанные с деятельностью преступников. В преступлениях с использованием IT-технологий при посягательстве на имущественную сферу потерпевшего, квалификация осуществляется не однозначно. В случаях, связанных с тайным хищением чужого имущества (ст. 158 УК РФ) [5] или осуществлением его посредством вымогательства (ст. 163 УК РФ) с использованием при этом неправомерного доступа к охраняемой законом компьютерной информации, квалификацию таких деяний необходимо дополнить статьями Уголовного кодекса РФ, защищающими компьютерную информацию (ст. 272, 273, 274, 274.1 УК РФ). Если преступная деятельность связана с мошенничеством, то квалификация усложняется разграничением мошенничества с использованием средств социальной инженерии, осуществляемое с использованием IT-технологий от кибермошенничества. Первый вид мошенничества предполагает психологическое манипулирование

людьми с целью совершения определенных действий или разглашения конфиденциальной информации [7], поскольку в данном случае не исключается использование рассылок (если они не привели уничтожению, блокированию, копированию или модификации компьютерной информации), размещения недостоверной информации в социальных сетях и других ресурсах сети Интернет. Отличительной чертой кибермошенничества (ст. 159.6 УК РФ), в свою очередь, являются последствия манипуляции с компьютерной информацией в форме уничтожения, блокирования, копирования или модификации компьютерной информации или иного вмешательства в функционирование средств хранения, обработки или передачи информации, или информационно-телекоммуникационных сетей, в остальном составы рассматриваемых преступлений идентичны, что и создает проблему при квалификации конкретных деяний. Дополнительное толкование относительно квалификации кибермошенничества дают положения пункта двадцатого Постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 “О судебной практике по делам о мошенничестве, присвоении и растрате: «…квалификация по статье 159.6 УК РФ будет осуществляться в случае, если имеет место целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, компьютеры (в т. ч. портативные), снабженные соответствующим ПО, или на информационно-телекоммуникационные сети, нарушающее установленный процесс хранения, передачи и обработки компьютерной информации и позволяющее преступнику незаконно завладеть чужим имуществом. Компьютерное мошенничество посредством неправомерного доступа и распространения вредоносных программ требует дополнительной квалификации по статьям 272, 273, 274.1 УК РФ.» Двадцать первый пункт того же Постановления в свою очередь определяет существенные признаки мошенничества (ст.159 УК РФ). Так, если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-

телекоммуникационных сетях, включая сеть «Интернет» (например, создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по статье 159, а не 159.6 УК РФ [12]. В пандемию COVID-19, согласно аналитическим данным Group-IB наиболее актуальными стали достаточно сложные с точки зрения состава преступления способы и методы реализации кибермошенничества [1]. Преступники активизировали атаки с использованием социальной инженерии, основанной на эксплуатации темы коронавируса во вредоносных рассылках и активного рекрутинга в преступные сообщества новых участников. Привлечение в преступные сообщества осуществлялись через телеграм-каналы и хакерские форумы, на которых обещали обучение.

Основным объектом атак кибермошенников являлась электронная почта [4], так как это один из самых популярных персональных информационных ресурсов, особенно в условиях его использования для дистанционной работы сотрудниками компаний, переведенными на дистанционную работу. Эксперты выявляли много замаскированных, в том числе и под сообщения о COVID-19, вложений с программами-шпионами. Также преступники осуществляли массовые рассылки о штрафах за нарушение карантина, поддельных цифровых пропусков, приглашений от имени сервиса видеоконференций Zoom и т.д. [9].

Квалификация подобных деяний осуществляется по ст. 159.6 УК РФ, так как помимо методов социальной инженерии при совершении преступления происходит манипуляция информацией в одной из форм, предусмотренных в пункте 1 этой статьи [4]. В случае применения вредоносного ПО или нарушения хранения, или обработки компьютерной информации необходима дополнительная квалификация по ст. 273, 274, 274.1 УК РФ. За прошедшие месяцы пандемии, согласно отчёта генерального директора компании Group-IB Ильи Сачкова, было заблокировано около 5000 фишинговых ссылок,

замаскированных способами, рассмотренными в примерах, в то время как такое же количество было зафиксировано суммарно за 2018 год [15].

Заключение

Исследование квалификации преступлений, с использованием IT-технологий в условиях пандемии COVID-19 позволяет выделить несколько характерных проблем, обострившихся в условиях кризисного явления и требующих конструктивного разрешения. Значительной проблемой для квалификации преступлений в сфере информационной безопасности является необходимость ее дополнения помимо статей главы 28 УК РФ «Преступления в сфере компьютерной информации» статьями, деяния субъектов в которых сопряжены с доступом к компьютерной информации, связанных с мошенничеством (ст. 159 УК РФ), посягательством на авторские и смежные права (ст. 146 УК РФ), незаконным оборотом специальных технических средств, предназначенных для негласного получения информации (ст. 138.1 УК РФ), кражей (ст. 158 УК РФ) и др. [3]. Представляется, что данная особенность обусловлена использованием информационных технологий, вредоносных программ прежде всего в качестве способа получения доступа к основному объекту посягательства. Так, квалификация исключительно по статье 273 УК РФ не осуществляется в силу использования вредоносных программ практически всегда для доступа к информации. Около 2% деяний квалифицируются по ст. 272 и 273 УК РФ, около 3% по ст. 273 и 146 УК РФ, примерно 5 % по статье 272 УК РФ [3]. Лидирующие позиции занимает одновременная квалификация по ст. 272 и 146 УК РФ-34%, по ст. 146,272,273 УК РФ-около 54% и по ст.159, 272, 273 УК РФ- примерно 60% [14]. В связи с этим, следует рассмотреть данную проблему с точки зрения оптимизации законодательства, посредством формулирования на основе статей главы 28 УК РФ квалифицирующих признаков преступлений, посягающих на собственность, конституционные права и свободы человека и др., исключив при этом положения статей главы 28 УК РФ и, соответственно, проблему необходимости дополнительной квалификации рассмотренных

составов правонарушений. С целью реализации данного предложения, содержание новых редакций статей глав 19 УК РФ «Преступления против конституционных прав и свобод человека и гражданина», 21 УК РФ «Преступления против собственности», и других составов преступлений, предполагающих возможность неправомерного доступа к компьютерной информации, следует дополнить пунктом части 2, содержащим следующие положения: « … Те же деяния, совершенные с получением неправомерного доступа к охраняемой законом компьютерной информации или нарушением правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, если это деяние повлекло уничтожение, блокирование, модификацию, копирование компьютерной информации или нейтрализацию средств защиты компьютерной информации, а равно сопряженное с созданием, распространением или использованием компьютерных программ или иной компьютерной информации в этих целях». Часть 3 соответствующих Глав и статей также необходимо дополнить пунктом: «…Деяния, предусмотренные пунктом «[предыдущий пункт]» части 2, воздействующие на объекты критической информационной инфраструктуры Российской Федерации…».

В период пандемии COVID-19 наиболее остро встала и проблема достоверности информации в сети Интернет, поскольку в условиях кризисного явления в обществе ложная информация всегда негативно влияет на настроения и дестабилизирует ситуацию в целом. Введение в действие новеллы уголовного права ст. 207.1 УК РФ, направленной на защиту общества от публичного распространения заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, представляется важным и свидетельствует о положительной динамике развития правового регулирования в информационной сфере, однако дополнительным

квалифицирующим признаком, по мнению автора, необходимо также считать и осуществление публичного распространения информации посредством сети «Интернет», вредоносного программного обеспечения, иного вмешательства в функционирование информационно-телекоммуникационных сетей, поскольку в условиях цифровизации такие способы распространения являются наиболее актуальными и требуют более жестких мер наказания по сравнению с предусмотренными в самой статье. Необходимой санкцией для IT-преступников в данной сфере, по мнению автора, в случае причинения значительного ущерба обществу, является лишение свободы до пяти лет.

В контексте проведенного исследования также была выявлена необходимость разграничения преступлений, совершенных посредством методов социальной инженерии, IT-технологий и киберпреступлений. В частности мошенничество с использованием методов социальной инженерии, IT-технологий в отличие от кибермошенничества могут осуществляться и при помощи IT-технологий, но не содержать квалифицирующего признака кибермошенничества- последствия доступа к охраняемой законом компьютерной информации, то есть ее уничтожения, блокирования, копирования или модификации. Таким образом, комбинирование способов и методов осуществления мошенничества при совершении преступниками реальных деяний усложняет или делает невозможным процесс их квалификации. Для решения данной проблемы в случае с мошенничеством достаточным следует считать реализацию предложения по модернизации законодательства путем формирования квалифицирующих признаков на основании главы 28 УК РФ в преступлениях, связанных с мошенничеством (ст. 159 УК РФ), а также увеличение наказания за данные правонарушения с целью повышения значимости охраны информационной безопасности. Оптимальной санкцией для IT-преступников в данной сфере, по мнению автора является ограничение свободы до 3-х лет, а в случае причинения значительного ущерба гражданину до шести лет лишения свободы. В таком случае необходимо также исключить

статью 159.6 УК РФ в силу утраты отсутствия необходимости в ее применении при наличии квалифицирующих признаков в ст. 159 УК РФ.

Библиографический список:

1. Group-IB назвала ключевые тенденции киберпреступлений в период пандемии.URL: https://www.group-ib.ru/media/covid-cybercrime-trends/.
2. Positive Technologies: Актуальные киберугрозы: II квартал 2020 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q2/.
3. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / [А. В. Аносов и др.]. – М.: Академия управления МВД России, 2019. – Ч. 1. – 208 с.
4. Карасёва М.Ю. Преступления в сфере компьютерных технологий. // Экономика и право. XXI век. 2012. № 4. С. 100-103.
5. Карасёва М.Ю. Криминологическая характеристика личности субъекта, совершающего преступления по неосторожности. // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2014. № 2. С. 102-107.
6. Карасёва М.Ю. Анализ прибыли предприятия ООО "МОСФРИЗ" и способы ее повышения // Экономика и предпринимательство. 2015. № 5-1 (58). С. 462-466.
7. Карасёва М.Ю. Криминологическая характеристика субъекта преступления. // Экономика и право. XXI век. 2013. № 1. С. 85-92.
8. Киберпреступность и распространение дезинформации во время пандемии COVID-19. URL:https://www.un.org/ru/coronavirus/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19.
9. Лаборатория Касперского. URL: www.kaspersky.ru.

10. Министерство внутренних дел Российской Федерации: состояние преступности. URL: https://xn--b1aew.xn--p1ai/reports/item/21551069/.

11. Портал правовой статистики Генеральной прокуратуры Российской Федерации. URL: https://genproc.gov.ru/stat/data/.

12. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 “О судебной практике по делам о мошенничестве, присвоении и растрате».

13. Уголовный кодекс РФ от 13 июня 1996 г. N 63-ФЗ (ред. от 31. 07.2020).

14. Уголовный кодекс РФ. Комментарий с путеводителем по судебной практике. Под редакцией д. ю. н., профессора А.И. Чучаева. 2018 г. С. 1215-1231.

15. Эксперты назвали тенденции киберпреступлений в период пандемии. URL: https://rg.ru/2020/10/23/eksperty-nazvali-tendencii-kiberprestuplenij-v-period-pandemii.html.