МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение
высшего образования «Уфимский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра уголовного права и криминологии

ДИПЛОМНАЯ РАБОТА

на тему **«УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (СТ. 159.6 УК РФ) (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ И ОПУБЛИКОВАННОЙ СУДЕБНОЙ ПРАКТИКИ)»**

Выполнил
Черепанов Арсений Николаевич
обучающийся по специальности
40.05.02 Правоохранительная деятельность
2019 года набора, 923 учебного взвода

Руководитель
Заместитель начальника кафедры уголовного права и криминологии, к.ю.н., полковник полиции
Нугуманов Азат Риммович

К защите _____
рекомендуется / не рекомендуется
Начальник кафедры _____ И.Р. Диваева
Дата защиты «___» _____ 2024 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

В современном мире компьютерные технологии играют ключевую роль, и это очень актуально. Киберпреступность представляет серьезную угрозу для законодательных и правоохранительных органов. В ходе выступления на цифровой конференции в Сеуле, бывший глава ООН Пан Ги Мун отметил рост угроз, связанных с информационными технологиями.

В мире и в России мошенничество считается одним из классических видов преступлений. В рамках цифровой эпохи мы наблюдаем неизбежное развитие и эволюцию мошенничества, которое приобретает дистанционный характер и переходит в виртуальную сферу.

Активное развитие и выявление характеристик преступлений в области компьютерной информации обязательно требует борьбы с мошенничеством, выявления методов предотвращения преступлений, а также идентификации личности преступника.

Цель и задачи работы. Целью настоящего исследования является уголовно-правовой анализ мошенничества в сфере компьютерной информации

Достижение поставленной цели предопределило необходимость решения следующих задач:

1) Отразить объективные и субъективные признаки мошенничества в сфере компьютерной информации;

2) Проанализировать субъективные признаки мошенничества в сфере компьютерной информации;

3) Провести отграничение мошенничества в сфере компьютерной информации от смежных составов преступлений;

Судебная практика, статистические данные и научные труды - все это аспекты, которые анализируются в рамках исследования, охватывающего уголовно-правовые нормы и специфику правоотношений.

ГЛАВА 1. ИСТОРИКО-СРАВНИТЕЛЬНАЯ И УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА

§ 1. Историко-правовая характеристика мошенничества в сфере компьютерной информации

В современном мире человек стал сталкиваться с новыми вызовами из-за использования высоких технологий в повседневной жизни. Криптовалюты, онлайн-покупки, безналичные расчёты и переводы, а также общение в интернете стали неотъемлемой частью жизни. Вместе с этим, увеличивается число преступлений в цифровой среде. Особый интерес вызывает развитие историко-правовых аспектов мошенничества в области компьютерных технологий.

В начале появления электронно-вычислительных машин, компьютерные преступления оставались в тени. В первые два десятилетия после создания первого цифрового компьютера в 1943 году, кибератаки были едва ли возможны. Ограниченный доступ к огромным электронным машинам был предоставлен немногим, не соединенным в сеть. Мало кто знал, как ими управлять, что делало угрозу почти невидимой.

В 1950-х годах был разработан новый метод под названием «телефонный фрикинг», который позволял «мошенникам» - людям, увлеченным работой с телефонами, - захватывать протоколы для удаленной работы инженеров связи. Благодаря этому им удавалось осуществлять бесплатные звонки и избегать оплаты междугородных звонков. Телефонные компании не могли справиться с этим явлением, и только в 1980-х годах практика была прекращена. С развитием интернета в 1969 году ситуация лишь усложнилась.

В 1979 году компьютерные преступления впервые произошли в США, где были зарегистрированы первые случаи такого рода преступлений в 1969 и 1973 годах. Компьютерная преступность стала связана с использованием всемирной информационной сети Интернет как средства преступления. В СССР также произошли случаи компьютерных преступлений, и в городе Вильнюсе было

зафиксировано первое преступление, причинившее ущерб в размере 80 тысяч рублей.

В 70-е годы XX века компактные компьютерные системы стали широко распространены среди пользователей благодаря толчку развитию информационных технологий. Появление сети Интернет и увеличение числа пользователей создало проблему обеспечения надлежащей защиты систем и государственных серверов. Защитные системы, задуманные для снижения киберпреступности, на самом деле лишь способствовали увеличению числа преступлений в сети, поскольку появились профессионалы и схемы взлома, созданные ими.

В одном из случаев специалисты по информационной безопасности крупных компаний сами осуществляли взлом. В США первое уголовное дело против консультанта по компьютерной информации банка было возбуждено за расшифровку систем защиты и перевод 10 млн. долларов на свой счет. Еще одно типичное преступление было совершено А.

В период активного развития информационных технологий в начале 90-х гг. XX века инициативная группа Интерпола сделала попытку создать общую классификацию преступлений. Эта инициатива нашла свое отражение в Будапештской конвенции Совета Европы 2001 года. Страны G7 до сих пор предпринимают усилия по унификации уголовного законодательства в области борьбы с распространением компьютерных преступлений. Большинство таких преступлений имеют тенденцию к транснационализации. К., для того чтобы избежать уплаты налогов в размере 620 тыс. долл. США, взломал электронную сеть и успешно осуществил свое преступление.

В СССР и позднее в России стала активно распространяться волна компьютерных преступлений. Первый случай такого преступления был зафиксирован в 1979 году в Вильнюсе, когда было похищено 80 тысяч рублей. Одним из первых крупных компьютерных преступлений в России считается кража на сумму 125,5 тысяч долларов США и планирование кражи еще более 500 тысяч долларов США в Внешэкономбанке СССР в 1991 году. Именно в этот

период отечественное законодательство впервые начало заниматься уголовно-правовым регулированием в области распространения и использования информационных технологий.

В 1991 году был предложен проект закона "Об ответственности за правонарушения при работе с информацией" в РСФСР. Этот закон предусматривал возможность привлечения к ответственности по различным статьям за нарушения связанные с информацией. Но этот закон не был принят из-за отсутствия необходимого законодательного поля. Затем было принято более 600 нормативно-правовых актов, касающихся информационно-телекоммуникационной сферы.

В 1992 году был принят Закон России о правовой охране программ для электронно-вычислительных машин и баз данных, в 1994 году - Гражданский кодекс, который содержит ряд норм, связанных с компьютерной информацией, в 1995 году - Федеральный закон об информации, информатизации и защите информации. 07 апреля 1994 года Россия официально признана страной, представленной в Интернете, в этот день был зарегистрирован домен RU, считающийся днем рождения Рунета, российского сегмента мирового виртуального пространства.

В 1996 году был принят Уголовный кодекс Российской Федерации, включающий отдельную главу о уголовной ответственности за преступления в области компьютерной информации. Эта глава в значительной степени повторяла нормы уголовных кодексов стран - участниц СНГ, принятых в то же время, и осталась практически неизменной до настоящего времени.

Сегодня мы можем отметить, что нормативное регулирование киберпреступлений на международном уровне оставляет желать лучшего. Организация Объединённых наций не установила общий стандарт в данной области. Появление такого стандарта становится практически невозможным из-за поддержки странами Совета Европы Будапештской конвенции 2001 года, которая является основным правовым актом по уголовному преследованию лиц, совершающих киберпреступления. Россия и другие страны столкнулись с

препятствиями в усовершенствовании законодательства из-за этого международного документа.

Активное участие и сотрудничество всех государств мира необходимы для эффективного противодействия угрозам киберпреступного мира, приобретающим транснациональный характер. Это ясно видно из истории развития уголовного законодательства в сфере предупреждения киберпреступлений.

В киберпреступности стали лидерами многие страны бывшего Советского Союза и Центральной Восточной Европы. После распада СССР наступили нестабильные социально-политические условия, которые предоставили удобную возможность для эффективной и мощной киберпреступной деятельности. Развитие киберпреступности содействовали отсутствие законодательных норм и сложная политическая обстановка. Ограниченные возможности легального трудоустройства и нестабильная экономическая среда побуждали высокообразованных и технологически компетентных людей использовать свои навыки для преступной деятельности в киберпространстве.

В конце 1990-х и начале 2000-х годов тысячи граждан присоединились к онлайн-преступным группам и их криминальной среде из-за преобладания чувства безнаказанности, что было прямым результатом первоначальной комбинации факторов в постсоветскую эпоху. Оператор ЭВМ из Санкт-Петербурга, Владимир Левин, был арестован в 1990-е годы за попытку украсть более 10 миллионов долларов США, взломав счета Citibank. Это событие предвещало известность России в области киберпреступности, поддерживаемую давней традицией российской организованной преступности.

С началом появления новой угрозы на законодательном уровне, возникли попытки регулировать ответственность за совершение преступлений в сфере компьютеров. В результате разработан проект Закона РСФСР «Об ответственности за правонарушения при работе с информацией» в 1991 году, который предусматривал различные виды ответственности за компьютерные преступления, такие как дисциплинарная, гражданско-правовая,

административная, уголовная. Однако этот закон так и не был принят из-за своей недоработанности. Впоследствии был принят ряд нормативно-правовых актов, касающихся регулирования информационно-телекоммуникационной сферы. В 1992 году принимается закон России о правовой охране программ для электронно-вычислительных машин и баз данных, в 1994 году был принят Гражданский кодекс РФ, который содержит ряд норм, связанных с компьютерной информацией[1]. В 1995 году - Федеральный закон от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации». В 2006 г. был принят закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Указанный закон содержит понятия информация, обладатель информации др. и действует до сих пор. Уголовный кодекс Российской Федерации принятый в 1996 г, содержал отдельную главу, которая регламентировала уголовную ответственность за преступления в сфере компьютерной информации. Следует отметить, что на тот момент редакция главы 28 УК РФ практически полностью воспроизводила нормативные положения уголовного кодекса стран - участниц СНГ, который был также принят в 1996 году. В 2012 году появился специальный состав мошенничества в сфере компьютерной информации ст. 159.6 УК РФ. До ее введения действовал Пленум ВС РФ от 27.12.07 г. № 51, который устанавливал квалификацию по совокупности статей 159 и 272 УК ,273 УК РФ, 274 УК РФ, 274.1 УК РФ[2]. В настоящее время действует Постановление Пленума ВС РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»[3]. Таким образом, были проанализированы причины возникновения компьютерных

[1] Гражданский кодекс Российской Федерации (ГК РФ) от 30 ноября 1994 № 51-ФЗ Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 17.06.1996, № 25, ст. 2954. Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

[3] Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». № 48 // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. – Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

преступлений, а также рассмотрен вопрос развития историко-правового аспекта мошенничества в сфере компьютерных технологий.

Подводя итог данного параграфа, следует отметить, что исторически, мошенничество в сфере компьютерной информации стало широко распространенным с развитием интернета и цифровых технологий. Кибермошенники используют различные методы и технологии для обмана пользователей и получения доступа к их личным данным, финансовым средствам и другим ценным информационным ресурсам.

В правовом плане, мошенничество в сфере компьютерной информации рассматривается как преступление и подпадает под законы о киберпреступности. В большинстве стран приняты законы, которые наказывают мошенничество в сфере компьютерной информации и предусматривают суровые наказания для виновных лиц.

§ 2. Объективные признаки мошенничества в сфере компьютерной информации

При анализе уголовно-правовой характеристики преступного деяния необходимо уделить внимание всем признакам, которые определяют состав преступления. Это ключевой момент, который позволяет понять, что делает действие преступным, и какие элементы входят в его структуру.

Важно подчеркнуть, общей теории уголовного права России следует, что состав преступления – это совокупность предусмотренных уголовным законом объективных и субъективных признаков, характеризующих общественно опасное деяние как преступление. При этом любой состав преступления обладает признаками, которые принято группировать по элементам состава: объекту, объективной стороне, субъекту и субъективной стороне. Эти элементы играют решающую роль в определении степени вины и наказуемости совершенного деяния. В результате, понимание состава преступления и его элементов является необходимым для эффективного применения уголовного законодательства и обеспечения справедливости в уголовном процессе.

Верное определение объективных и субъективных признаков позволит правильным образом квалифицировать деяние преступника и соответственно верно назначить уголовное наказание. Более того, верное установление признаков способствует тому, что правоприменитель будет в состоянии отграничить одно преступное деяние от другого.

Процесс установления признаков преступления является сложным и требует глубоких знаний и опыта. Объективные признаки основываются на наблюдаемых фактах и доказательствах, в то время как субъективные признаки связаны с мотивами и намерениями преступника. Правильное понимание и анализ всех аспектов преступления позволяют судебным органам принимать обоснованные решения.

Корректная классификация преступлений и назначение соответствующего уголовного наказания обеспечивают справедливость и порядок в обществе. Именно поэтому важно уделять должное внимание определению признаков преступлений и строго следовать закону при их квалификации.

Объективные признаки состава преступления - это ключевые характеристики, которые включают в себя как объективную сторону, так и объект преступления. Понимание того, что является объектом преступления по статье 159.6 УК РФ, требует специального внимания и изучения.

Важно учитывать, что объект преступления имеет широкое определение, описанное в части 1 статьи 2 УК РФ. Там указывается, что объектом преступления могут выступать права и свободы человека и гражданина, собственность, общественный порядок и общественная безопасность, окружающая среда, конституционный строй Российской Федерации, мировая безопасность человечества. Эти аспекты являются важными при определении объекта преступления. Для более полного понимания данной темы необходимо учитывать структуру УК РФ, которая выделяет общий, видовой и непосредственный объекты преступления.

Важно понимать, что в названии разделов УК РФ указывается родовой (специальный) объект преступлений, тогда как главы УК РФ определяют видовой

(групповой) объект преступлений. Это означает, что родовой объект определяет группу однородных общественных отношений, которые охраняются уголовно-правовыми нормами определенного раздела УК РФ. Родовой объект является основой для определения конкретных видов преступлений, которые могут ущемлять эти общественные отношения. В свою очередь, видовой объект преступлений определяется характером непосредственного воздействия преступного деяния на общественные отношения, относящиеся к родовому объекту. Таким образом, различие между родовым и видовым объектами преступлений является ключевым аспектом системы уголовного законодательства.

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.

Целью данных преступлений является обман пользователей. Происходит хищение конфиденциальных данных, у мошенников появляется доступ к личной информации.

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 него.

Объективная сторона мошенничества в сфере компьютерной информации выражается в хищении чужого имущества, 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), а равно приобретения им юридического права на распоряжение такими деньгами (имуществом).

Кибермошенничество - это один из видов киберпреступлений, целью которого является причинение ущерба путем воровства личной информации. В основном его делят на пять видов. Все они направлены на получение персональных данных с целью перевода средств с персональной карты пользователя на другую или получения прямого доступа к персональному счету через сервисы онлайн-банкинга.

Вопрос о предмете мошенничества в области компьютерной информации является сложным и вызывает дискуссии. Согласно точке зрения В. И. Гладких, определить объект и суть преступления, указанного в статье 159.6 УК РФ, представляется крайне затруднительным[1]. Этот аспект сталкивается с противоречием, так как общепринятое представление о прямом объекте мошенничества как определенной форме собственности не совпадает с текущей формулировкой компьютерного мошенничества.

Статья 159.6 УК РФ относится к разделу VIII «Преступления против собственности», что позволяет определить общественные отношения, защищающие право собственности граждан, как родовой объект данной категории преступлений. Однако, когда дело касается сферы компьютерной информации, вопрос об объекте преступного посягательства становится сложным.

Сфера компьютерной информации охватывает другие области общественных отношений, подверженных воздействию преступлений, описанных в главе 28 УК РФ «Преступления в сфере компьютерной информации». Различия в определении объекта мошенничества в этой сфере и в

[1] Гладких В.И. Компьютерное мошенничество: а были ли основания для криминализации? // Рос. следователь. 2014. № 22. С. 25.

сфере общественных отношений охраны собственности граждан могут создавать противоречия в интерпретации закона и преследовании преступлений.

В современном мире с развитием информационных технологий возникла новая угроза - компьютерное мошенничество. Это преступление имеет двойной объект. Основным объектом являются общественные отношения, связанные с собственностью, в то время как дополнительным объектом выступают правоотношения, обеспечивающие информационную безопасность.

В условиях постиндустриального общества и широкого использования высоких технологий, по мнению А. Г. Безверхова, растет вероятность совершения компьютерного мошенничества[1]. Это деяние угрожает не только личной информационной безопасности, но и общественной безопасности в целом.

Таким образом, с увеличением числа технологических преступлений, необходимо уделять особое внимание защите информации и предотвращению угрозы, которую представляет собой компьютерное мошенничество. Важно развивать меры контроля и соблюдения законодательства в области кибербезопасности.

Существует неоднозначность в определении объекта преступления, предусмотренного статьей 159.6 УК РФ, согласно О. М. Сафонову[2]. Он указывает на то, что это преступление нарушает общественные отношения как в сфере собственности, так и в сфере безопасности компьютерных систем. По мнению автора, это преступление является двуобъектным, где основным объектом являются отношения собственности, а дополнительным – отношения в сфере безопасности компьютерных систем.

Однако в научной общественности существует иной подход к определению объекта данного преступления. Различные ученые и исследователи высказывают

---

[1] Безверхов А. Г. Мошенничество и его виды: вопросы законодательной регламентации и квалификации // Уголовное право. 2015. № 5. С. 8.

[2] Барчуков В. К. К вопросу о содержании признаков объективной стороны мошенничества в сфере компьютерной информации // Безопасность бизнеса. 2016. № 5.С. 41–46.

мнения о том, какие именно отношения оно нарушает и каковы его основные и дополнительные объекты.

Изучение данной проблемы требует дальнейшего анализа и исследований. Возможно, в будущем будут предложены новые точки зрения на определение объекта статьи 159.6 УК РФ и его места в системе уголовного законодательства.

Исходя из мнения Т. М. Лопатиной, важно осознать, что компьютерное мошенничество не только затрагивает отношения, связанные с правом собственности, но и оказывает влияние на общественные взаимоотношения в сфере компьютерной информации[1]. По мнению Т. М. Лопатиной, непосредственным объектом компьютерного мошенничества являются отношения, охраняющие право собственности, в то время как общественные отношения в сфере компьютерной информации являются факультативным объектом.

Важно отметить, что неправомерный доступ и модификация компьютерной информации не всегда являются обязательным признаком данного вида преступления. Существует множество других аспектов, которые также могут быть учтены при рассмотрении случаев компьютерного мошенничества.

Таким образом, необходимо учитывать широкий спектр разновидностей компьютерного мошенничества, а также тонкости и нюансы, которые могут возникать при качественной оценке ситуации. Важно разбираться в теме компьютерной безопасности и быть готовым к эффективной защите от подобных преступных действий в современном цифровом мире.

Рассмотрим подробнее современные способы совершения кибермошенничества:

1. Вид мошенничества, который сейчас активно распространен, представлен вирусами. Они способны заразить память устройства или другие программы для нарушения функционирования или кражи конфиденциальных

[1] Лопатина Т. М. Проблемы уголовно- правовой защиты сфер компьютерной информации: современный взгляд на мошенничество // Право и безопасность. 2013. № 3-4 (45). С. 98.

данных. Путь, по которому вирус может попасть на компьютер - через случайный файл, вредоносный сайт или электронное письмо. Когда пользователь пытается войти в банковский аккаунт, вводя одноразовые пароли, вирус выдает фальшивое сообщение о старом пароле. Таким образом, вирус может получить доступ к банковскому аккаунту и полностью контролировать его.

Для предотвращения кибермошенничества банковские специалисты рекомендуют принять несколько мер безопасности. Важно подключить СМС-подтверждение к карточному счету, постоянно проверять его состояние, не разглашать банковские данные на веб-ресурсах, активно использовать антивирусное ПО и, если возможно, создать виртуальную карту. Виртуальные карты обеспечивают такую же функциональность, как обычные пластиковые, но обладают дополнительной безопасностью благодаря возможности установки ограничений на сумму трат. Поэтому, даже если злоумышленники сумеют списать деньги, они смогут это сделать лишь в пределах установленного лимита.

2. Специалисты финансовой сферы рекомендуют принимать меры по защите от кибермошенничества, такие как постоянный контроль за состоянием карточного счета, использование СМС-подтверждения, осторожность при предоставлении персональных данных и регулярное обновление антивирусного ПО. Также можно создать виртуальную банковскую карту с ограничением максимальной суммы трат, чтобы минимизировать возможные потери от мошеннических действий.

3. Программа-вымогатель - вредоносное ПО, которое зашифровывает файлы на компьютере и блокирует доступ к системе, требуя выкуп за их разблокировку.

4. Фишинг - вид мошенничества в интернете, который направлен на кражу конфиденциальных данных, таких как личная информация, пароли, данные кредитных и дебетовых карт и др. Часто злоумышленники создают фальшивые сайты, чтобы обмануть пользователей и получить доступ к их личным данным.

Путем изменения адреса отправителя, показываемого у получателя писем, осуществляется рассылка сообщений на электронную почту, похожих на

сообщения известной и надежной организации или контакта. Мошенники выполняют атаку, вредоносный файл, содержащий фишинговое программное обеспечение, прикрепляется к письму, а также путем ссылок, переходя по которым пользователь попадает на опасный веб-сайт. В результате заражается компьютер, смартфон или другие устройства, и злоумышленник получает все данные для последующего мошенничества и кражи денег.

Под разными предлогами жертвам предлагают перейти по ссылке, мошенники используют различные способы обмана. Один из таких способов - отправка фальшивых писем от лица крупных банков, в которых говорится об изменениях в безопасности, блокировке карты или попытке воровства средств. Злоумышленникам интересны номер карты, ПИН-код, CVV/CVC. Под влиянием заблуждений или страха пользователи часто передают эту информацию.

При посещении сайта «банка» пользователь может стать жертвой фишинга, когда злоумышленники получают доступ к его личным данным и могут злоупотребить ими. Через фишинговые программы, установленные на устройстве пользователя, мошенники могут перенаправить его на поддельный сайт, где автоматически крадут конфиденциальную информацию.

Мошенники также часто используют метод копирования сайтов известных интернет-магазинов, чтобы получить данные банковских карт пользователей и похитить их деньги.

5. Мошенничество само по себе является последним видом кибермошенничества, представляющим серьезную угрозу в онлайн-мире. Например, существуют разнообразные курсы и финансовые пирамиды, которые обещают быстрое обогащение и заработок, но на самом деле являются обманом.

С учетом увеличения числа жалоб от граждан, ставших жертвами противоправных действий в сети, а также повышения технической и юридической грамотности преступников, можно сделать печальный вывод, что существующие меры противодействия мошенничеству в интернете недостаточны.

Вопрос о характере преступления требует более детального рассмотрения. Для этого полезно обратиться к постановлению Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»[1]. Важным пунктом является пункт 20, который подчеркивает нарушение установленного процесса обработки, хранения и передачи компьютерной информации путем вмешательства в соответствующие средства. Это действие рассматривается как серьезное преступление, и именно такую точку зрения поддерживает судебная практика, основываясь на данных из анализа судебных дел за 2020 год.

Злоупотребление доступом к компьютерной информации или нарушение процесса ее обработки – это проблемы, требующие особого внимания в современном информационном обществе. Понимание того, как именно закон определяет такие действия как преступление, позволяет эффективнее бороться с ними. Важно понимать, что даже кажущиеся незначительными нарушения могут иметь серьезные последствия для безопасности в цифровом пространстве.

Безопасность данных и защита информации – это одни из ключевых аспектов современного правопорядка. В свете актуальной судебной практики необходимо постоянно совершенствовать законодательство и методы борьбы с преступлениями в сфере информационных технологий. Уголовная ответственность за нарушения в области компьютерной информации помогает обеспечить надлежащий уровень защиты данных и предотвращение преступлений в этой области.

Подробное исследование преступлений, совершаемых через модификацию информации в электронных системах, показало, что злоумышленники активно использовали уязвимости в платежных системах, базах данных и электронных ресурсах. Один из примеров из документов системы ГАС «Правосудие» описывает ситуацию, где хакер незаконно получил доступ к модулю SBMS для

[1] Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». № 48 // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

изменения данных об абонентских операциях клиентов ПАО «данные изъяты», выбрав абонентский номер без согласия владельца.

Подобные инциденты заставляют задуматься о том, что такие действия несут двойную угрозу: как для защиты личных данных клиентов, так и для безопасности самой системы. Именно поэтому преступления такого рода можно рассматривать как явление с двойным объектом воздействия.

Исследование продолжается, и важно учитывать, что технологии развиваются быстрее, чем механизмы защиты от киберпреступности. Вместе с тем, обнаружение и предотвращение подобных инцидентов требует комплексного подхода, который сочетает в себе как технические меры безопасности, так и обучение персонала правилам работы с конфиденциальной информацией.

С развитием технологий в мире возникает срочная необходимость в обеспечении безопасности данных. Ежедневно увеличивается роль защиты информации от угроз и взломов. Необходимо отметить, что главным объектом в данном контексте являются общественные связи, касающиеся собственности независимо от ее формы. Другим важным аспектом являются правовые отношения, направленные на обеспечение безопасности данных. Эти два компонента тесно связаны между собой и играют важную роль в обеспечении стабильности в области информационных технологий. Сохранение конфиденциальности информации и предотвращение несанкционированного доступа имеют ключевое значение в области информационной безопасности.

При обсуждении возможности электронных денежных средств как объекта преступлений и права, предмет рассмотрения в области компьютерной информации становится центром внимания в исследовании объективных признаков мошенничества. На втором месте по спорным вопросам возникает обсуждение.

Согласно ученому М. А. Коростелеву, объектом права собственности не могут быть признаны безналичные и электронные деньги. В уголовной и гражданской науке существует разнообразие точек зрения на этот вопрос.

Поэтому необходимо провести дальнейший анализ и обсуждение, чтобы прояснить этот аспект и разрешить возможные противоречия и неоднозначности в правовой области.

В современной экономике ключевую роль играют безналичные средства и электронные деньги, обеспечивая удобство и эффективность в финансовых операциях. Безналичные денежные средства, цифровые права и бездокументарные ценные бумаги определяются статьей 123 Гражданского кодекса РФ как имущественные объекты гражданских прав[1]. Электронные деньги и цифровые активы представляют собой новые направления развития финансовых инструментов, которые отвечают современным требованиям.

С каждым днем увеличивается число финансовых преступлений и мошенничества, чему способствует растущий интерес к электронным деньгам и ценным бумагам без бумажного оформления. Преступники активно используют эти средства, так как они предоставляют удобную возможность для осуществления незаконных действий.

В современном мире защита цифровых активов и электронных денег становится ключевым элементом в борьбе с финансовыми преступлениями. Новые методы обеспечения безопасности финансовых интересов граждан и противодействия незаконному использованию платежных средств требуются правоохранительным органам в условиях быстрого развития технологий. Законы и нормативные акты играют важную роль в защите финансовых операций и интересов бизнеса и населения, поэтому их значимость неоспорима. Для обеспечения надежности финансовых транзакций крайне важно создать и внедрить эффективные механизмы контроля за электронными средствами.

С развитием технологий и увеличением интереса к криптовалютам, крайне важно строго соблюдать законы, чтобы предотвратить возможные преступления и злоупотребления. В связи с этим, регулирование и определение статуса

[1] Гражданский кодекс Российской Федерации (ГК РФ) от 30 ноября 1994 № 51-ФЗ Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

криптовалют начинают играть все более значимую роль, требуя внедрения соответствующих мер и контрольных механизмов.

Для достижения более эффективной стратегии защиты и профилактики финансовых преступлений и предотвращения их различных форм, необходимо разработать меры, которые будут более эффективно бороться с нарушениями финансового законодательства, связанными с кражей электронных средств. Преступники могут использовать компьютерные данные для незаконного получения денег и ценных бумаг, таких как билеты на транспорт или в театр.

Процесс удаления информации не всегда означает её полное и окончательное уничтожение, что поднимает вопросы о надёжности данной процедуры.

Следовательно, вопрос удаления информации с компьютера оказывает прямое влияние на безопасность данных и конфиденциальность информации. Законодательство оговаривает правила и нормы в отношении удаления информации, но оставляет место для различных интерпретаций и возможных уязвимостей в процессе удаления.

Кроме того, научное сообщество и правовые эксперты активно обсуждают понятие «иное вмешательство» в компьютерные данные, предлагая различные точки зрения и подходы к данной проблеме. Неопределенность в уголовном законе позволяет обсуждать и уточнять нормы по защите информации, что может привести к разработке более точных правил в области информационной безопасности.

Таким образом, как было упомянуто, указанные действия направлены на информацию, хранящуюся на компьютере. В то же время законодательство подразумевает возможность иного вмешательства, не уточняя его суть. В связи с отсутствием четкого определения данного понятия в уголовном законе, юридическая наука предлагает различные точки зрения на виды такого вмешательства.

Так, большинство исследователей сходятся во мнении в том, что иное вмешательство следует расценивать, как любое воспрепятствование

нормальному процессу функционирования информационной или информационно-телекоммуникационной сети.

Однако эта позиция не является единственной и, анализируя научные публикации можно также встретить мнение о том, что иное вмешательство предполагает также и любое незаконное воздействие на проводимые в отношении информации процессы, которые мешают ее нормальному использованию. Более того, ученые согласны в том, что чаще всего иные вмешательства происходят с применением ввода, однако не исключены и другие методы.

Как известно, мошенничество предполагает наличие такого признака, как обман. Обман в свою очередь подразумевает сообщение или предоставление кому-либо тех сведений, который не отвечают действительности. На основании предоставления таких сведений происходит введение в заблуждение потерпевшего лица. Стоит при этом подчеркнуть, что многие авторы говорят об отсутствии признака обмана применительно к мошенничеству в сфере компьютерной информации, поскольку как таковой потерпевший в этом посягательстве отсутствует именно относительно введения его в заблуждение. Специфика данного преступления несколько иная – не происходит обман или злоупотребление доверием потерпевшего – атаке подвергаются определенные информационные системы.

Мошенники всегда ищут новые способы обмана, а с развитием технологий возможности для мошенничества расширяются. Это подтверждает необходимость постоянного повышения информационной грамотности и бдительности в онлайн-среде.

Борьба с мошенничеством требует совместных усилий государства, бизнеса и общественности. Важно развивать системы защиты от мошенничества и обучать людей распознавать и предотвращать подобные преступные действия.

В современном мире, где информационные технологии занимают все более важное место, преступления против информационных систем становятся все более актуальными. Важно понимать, что они имеют свою специфику, отличную

от обычных преступлений, где чаще всего присутствует элемент обмана или злоупотребления доверием. В данном случае, атаке подвергаются сами информационные системы, что вызывает серьезные последствия как для частных лиц, так и для компаний и государств.

О чем более подробно будет рассмотрено далее. Однако стоит здесь согласиться с мнением М.В. Степанова, который справедливо отмечает: «о каком обмане или злоупотреблении доверием можно вести речь, если отсутствует лицо, которому сообщаются ложные или несоответствующие действительности сведения».

При рассмотрении способа совершения таких преступлений стоит отметить, что он может быть схож с тем, что применяется в других областях преступной деятельности. Однако здесь ключевым фактором является не столько манипуляция с людьми, сколько манипуляция с самой информацией, что делает эти преступления особенно хитрыми и опасными для общества в целом.

Для более глубокого понимания методов совершения преступлений, связанных с компьютерными системами, необходимо изучить различные способы, такие как ввод, удаление, блокирование или модификация информации. Эти действия составляют основу преступлений против информационной безопасности. Один из наиболее типичных способов совершения преступлений, описанных в статье 159.6 УК РФ, - это вмешательство в корпоративные базы данных компаний.

Для изучения таких методов преступлений необходимо также изучить способы защиты от них. Это включает в себя использование шифрования данных, установку межсетевых экранов, антивирусное программное обеспечение, а также регулярное обновление программного обеспечения и обучение персонала компании правилам информационной безопасности. Только понимая, каким образом преступники могут совершать преступления в сфере информационной безопасности, можно эффективно защищаться от них и предотвращать утечку и кражу информации.

Подводя итог данного параграфа следует отметить, что объективные признаки мошенничества в сфере компьютерной информации включают следующие способы совершения преступления:

Ввод, удаление, блокирование, модификация компьютерной информации.

Иное вмешательство, которое влечёт за собой последствия в виде причинения ущерба субъектам права.

Мошенничество в сфере компьютерной информации посягает в первую очередь на отношения против собственности, но также затрагивает и правоотношения, обеспечивающие информационную безопасность.

§ 3. Субъективные признаки мошенничества в сфере компьютерной информации

Субъект преступления, как важный элемент состава преступления, несет в себе не только объективные, но и субъективные признаки, что делает его особенно значимым для правоприменительной практики. Каждое преступление имеет своего субъекта и субъективную сторону, которые необходимо учитывать при вынесении судебного решения.

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 вменяемое физическое лицо, достигшее 16 лет.

Осознание того, что субъект преступления объединяет признаки, характеризующие исполнителя противоправного деяния, является ключом к пониманию мотивов и целей преступника. Эта информация имеет большое значение в процессе расследования, установления виновности и определения наказания.

Для определения субъекта преступления важно учитывать различные признаки, такие как физическая природа, возраст, вменяемость и специальные

характеристики. Физическое лицо, признание гражданина вменяемым и достижение требуемого возраста - все эти факторы необходимы при анализе субъекта преступления.

Необходимо также обратить внимание на возраст субъекта. Согласно части 1 статье 20 Уголовного кодекса РФ, общий возраст субъекта составляет 16 лет. Эти критерии субъекта являются общими и применимы для всех составов преступлений, предусмотренных законодательством.

При анализе личности преступника также важно учитывать его социальный статус, образ жизни, возможные мотивы и даже психологические особенности. Для осознания полной специфики мошенничества в области компьютерных данных, необходимо погрузиться в их уникальные аспекты. Хотя формы мошенничества, такие как кража и приобретение собственности, остаются неизменными, способы их выполнения становятся все более специфическими.

Для того чтобы привлечь к уголовной ответственности за совершение преступлений, важно учитывать возраст. Возраст шестнадцать лет считается критическим в этом вопросе. Национальность обвиняемого не играет роли, так как возраст является универсальным фактором ответственности перед законом.

Рассматривается активный вопрос о снижении возрастного порога уголовной ответственности за мошеннические действия в уголовной науке. Основываясь на анализе последствий и эффективности потенциального изменения законодательства, поддерживается предложение. Важно отметить, что при рассмотрении уголовной ответственности лиц, которые превысили возраст в шестнадцать лет, необходимо анализировать конкретную ситуацию.

Важно учитывать общие правовые принципы, возраст и другие соответствующие аспекты при оценке справедливости ответственности и установлении критериев вины.

В наше время возраст уголовной ответственности становится все более обсуждаемым и актуальным в обществе. Разнообразные точки зрения на этот вопрос поднимаются, но нужно учитывать множество аспектов. Согласно

предложениям С. С. Медведева, возраст уголовной ответственности за мошенничество может быть снижен до 14 лет, основываясь на ускоренном процессе социализации и отсутствии необходимости визуального контакта с жертвой в области высоких технологий[1].

Подозрения и негодование вызывает данный аргумент по различным причинам. При установлении возрастного предела уголовной ответственности необходимо учитывать способность несовершеннолетних адекватно воспринимать и оценивать разнообразные законодательные нормы.

Важно провести детальное исследование в данной сфере, учитывая не только изменения в технологиях, но и особенности социокультурного контекста нашего современного общества. Дискуссия о том, в каком возрасте следует привлекать к уголовной ответственности за мошенничество, требует всеобъемлющего изучения и обсуждения с целью найти оптимальное решение, учитывающее все аспекты проблемы и защищающее интересы несовершеннолетних и общества в целом.

В области уголовного права значительным фактором является способность осознавать и контролировать свои действия - это так называемая вменяемость, которая может быть рассмотрена с точки зрения не только медицины, но и психологии, социологии и философии.

Когда дело касается привлечения к уголовной ответственности, ключевым фактором становится понимание того, что психическое состояние и осознание действий человека могут колебаться в зависимости от обстоятельств. Поэтому важно учитывать понятие вменяемости, которое имеет определяющее значение в уголовном праве.

Важно учитывать, что оценка вменяемости зависит от множества факторов и может быть проведена специалистами различных профилей, учитывая различные аспекты личности и поведения. Для обеспечения справедливого и

---

[1] Дворецкий М. Ю. Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики // Вестник ТГУ. 2013. № 8 (124). С. 407.

точного рассмотрения вопросов вменяемости необходимо провести тщательный анализ и принимать информированные решения.

В российском уголовном законодательстве существует важное понятие - некомпетентность. Если человек не соответствует критериям компетентности или был некомпетентным в момент совершения преступления, он не может быть привлечен к уголовной ответственности. Часто такая ситуация возникает в отношении статей Уголовного кодекса, связанных с мошенничеством, например, статья 159.6. Некомпетентность может быть вызвана различными факторами, такими как психические расстройства или умственная отсталость. Важно отметить, что это понятие не имеет точного соответствия в уголовном законодательстве, и это может привести к серьезным правовым последствиям для всех участников уголовного процесса.

Важно отметить, что для возможности привлечения лица к уголовной ответственности необходимо убедиться, что лицо осознавало свои действия и понимало возможные последствия. Поэтому ключевую роль в рассмотрении уголовного дела играет экспертное заключение о вменяемости в момент совершения преступления. Определение психического состояния лица через экспертное заключение о невменяемости является значительным в этом контексте. Однако также важно учитывать вменяемость лица в момент совершения преступления. Наличие экспертного заключения необходимо для процесса привлечения к уголовной ответственности.

Для обеспечения справедливости и законности в уголовном процессе необходимо проведение судебной экспертизы, чтобы определить психологическое состояние подсудимого. В соответствии с Уголовно-процессуальным кодексом, это обязательный этап в случаях, когда возникают вопросы о способности подсудимого эффективно защищать свои права. Решения суда могут быть нравственно недостоверными, если не провести оценку психического состояния подозреваемого. Оценка психики обвиняемого имеет важное значение для правосудия, поэтому проведение экспертизы является

критическим шагом для обеспечения справедливости и защиты всех участников судебного процесса.

В сегодняшнем мире проведение судебно-психиатрической экспертизы обретает высокий статус, поскольку не только физические действия, но и умелые интеллектуальные манипуляции способны вызвать общественное беспокойство. Преступления в области цифровой информации требуют особых усилий и глубокого анализа со стороны специалистов в данной области. Например, в связи с заключением судебно-психиатрической комиссии экспертов № 2495 от 03.10.2018, принимается во внимание, что Соловьев С.Н. был способен осознавать характер и последствия своих действий как в момент совершения преступления, так и на данный момент, и не нуждается в принудительных медицинских мерах[1].

Экспертиза играет ключевую роль в определении умысла и способности человека к пониманию социальной реальности. Сложность современных преступлений требует глубокого понимания не только их физической, но и психологической природы. Понимание психического состояния подсудимого является одним из важных аспектов судебного процесса, особенно в контексте развития цифровых технологий и киберпреступности.

Психологический возраст субъекта преступления, описанного в статье 159.6 УК РФ, становится важным аспектом в определении уголовной ответственности. Помимо календарного возраста, который определен законом, существует также психологический возраст, упомянутый в части 3 статьи 20 УК РФ. Это означает, что несовершеннолетний, достигший возраста уголовной ответственности, но находящийся на заднем плане по психическому развитию, не имеющему отношения к психическому расстройству, как показано судебной комплексной психолого-психиатрической экспертизой, может не осознавать полностью характер и общественную опасность своих действий или бездействий

[1] Дворецкий М. Ю. Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики // Вестник ТГУ. 2013. № 8 (124). С. 407.

и, следовательно, не подлежать уголовной ответственности. Отметим, что данное положение закона направлено на обеспечение справедливости и учета индивидуальных особенностей каждого рассматриваемого случая.

Оценивать последствия своих поступков пока еще не способен ребенок, лишенный жизненного опыта, который присущ его сверстникам. Это делает его «невменяемым по возрасту» с психической точки зрения. Стоит отметить, что при рассмотрении совершения действий, предусмотренных законом, в частности, ст. 159.6 УК РФ, важно помнить о возможном участии лица, занимающего служебное положение, в данном контексте. Важно привлечь внимание к факту, что лицо, которое занимает определенную должность, является одним из ключевых участников рассматриваемого преступления.

Следует также подчеркнуть, что психическое здоровье ребенка играет важную роль в его способности понимать и осознавать последствия своих действий. Недостаток жизненного опыта и социальных навыков может привести к невменяемости по возрасту, что требует особого внимания и понимания. Поэтому необходимо учитывать индивидуальные особенности каждого случая, особенно при рассмотрении статей уголовного кодекса, требующих специфического подхода к лицам, занимающим определенные позиции.

Важно отметить, что в контексте пункта 29 Пленума Верховного Суда Российской Федерации № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» не требуется, чтобы должностное лицо имело непосредственный доступ к управлению денежными средствами[1]. Вмешательство с целью получения финансовой выгоды может оказаться вторичным по отношению к изменениям, вносимым в электронную отчетность и базы данных, однако само внесение изменений должно быть направлено на личную выгоду. На практике это может проявиться в таких случаях, как изменение данных о выполнении физической подготовки военнослужащих

[1] Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». № 48 // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. – Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

военной части под видом повышенного уровня квалификации, что впоследствии приводит к незаконным выплатам.

Перед тем, как приступить к анализу субъективной стороны преступления, необходимо обратить внимание на внутренние мотивы и чувства обвиняемого. Такой аспект отражает его психологическое состояние и отношение к тому, что он совершил. Субъективная сторона преступления означает именно ту внутреннюю реакцию субъекта на совершаемое им деяние, которая возникает в момент его совершения.

Подробное изучение субъективной стороны позволяет понять, как преступник воспринимает свои поступки и какие мотивы его двигали. Не стоит забывать, что не все психические состояния могут быть признаны как часть субъективной стороны преступления. Рассматривать лицо только через призму его психики недостаточно для полного понимания происходящего. Важно также учитывать социокультурный и личностный контекст, влияющий на субъективное восприятие действий преступника.

Крайне важно отметить здесь тот факт, что не любое психическое состояние лица при оценке содеянного будет рассматриваться, как субъективная сторона. Рассмотрение особенностей психики субъекта затрагивает лишь тот временной промежуток, в рамках которого совершалось преступное деяние. Как правило, субъективная сторона состоит из нескольких элементов, куда входят вина, мотив и цель, которыми руководствовался преступник. Однако мотив и цель являются факультативными признаками и их установление требуется не всегда. Определению мотива и цели стоит уделять особое внимание в том случае, когда в норме Особенной части УК РФ эти аспекты выступают в роли квалифицирующих признаков. Относительно рассматриваемого посягательства следует отметить, что мотив и цель при оценке содеянного не имеют значения, поскольку более серьезное наказание за их наличие в ст. 159.6 УК РФ не предусмотрено.

В современном мире компьютерное мошенничество становится все более распространенным и сложным преступлением. Рассмотрим субъективную

сторону этого явления, которая выражается в умышленной вине виновного лица. В уголовном праве возникает вопрос о том, какой вид умысла присутствует при совершении подобных преступлений. М. Ю. Дворецкий считает, что деяния, предусмотренные законодательством, относятся к умышленным и могут быть совершены с различными формами умысла[1].

Компьютерное мошенничество, как и любая другая форма хищения, связано с корыстной целью. Это означает, что виновное лицо стремится либо обогатиться самому, либо обогатить других лиц за счет чужого имущества, нарушая установленный законом порядок распределения материальных благ. Преступники используют различные технологии и методы, чтобы добиться своих корыстных целей, что делает их действия еще более опасными и трудно раскрываемыми. В связи с этим важно принимать меры для защиты информации и предотвращения подобных преступлений.

Когда преступник осознает, что его действия считаются преступными, он понимает, что за них последует наказание по закону. Важным фактором здесь является волевой критерий, который подразумевает, что преступник имеет умысел и желание, чтобы его действия привели к общественно-опасным последствиям.

В контексте корыстной цели возникает спорный вопрос в юридической науке: является ли изъятие чужого имущества корыстным деянием, если нет намерения использовать его в своих интересах, например, передать другим лицам или уничтожить кредитные обязательства.

Следует также учитывать, что понятие корысти может иметь разные интерпретации в различных ситуациях и контекстах. Для раскрытия корыстной цели необходимо анализировать не только намерения преступника, но и возможные последствия его действий и цели, которых он хочет достичь.

---

[1] Дворецкий М. Ю. Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики // Вестник ТГУ. 2013. № 8 (124). С. 40.

При рассмотрении дел о мошенничестве, присвоении и растрате, суды должны учитывать обязательный признак хищения - корыстную цель. Это означает, что виновный стремится изъять или присвоить чужое имущество для личной выгоды или передачи другим лицам, на которых у него есть какой-то интерес, будь то симпатия, сострадание или бравирование. Такую позицию отстаивает Л. В. Иногамова-Хегай[1].

Важное значение корыстной цели при совершении мошенничества в сфере компьютерной информации подчеркивается также в постановлении Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»[2]. Суды вынуждены учитывать, что хищение имущества возможно только при наличии у лица желания извлечь выгоду из чужого имущества, включая передачу его третьим лицам, которых не ограничивает определенный круг.

Делая вывод по данному параграфу, отметим, что субъективная сторона данного преступления предполагает прямой умысел. Виновный осознает, что завладевает чужим имуществом или правами на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Обязательным признаком является и корыстная цель, которая, как мы убедились, свойственна всем составам мошенничества.

Субъект мошенничества в сфере компьютерной информации - общий, по части 3 статьи 159.6 УК РФ - специальный, квалифицирующим признаком выступает совершение преступления группой лиц по предварительному сговору либо организованной группой.

---

[1] Иногамова-Хегай Л. В. Мошенничество, присвоение, растрата: проблемы квалификации конкурирующих и смежных норм // Уголовное право. 2015. №5. С. 30 – 34.

[2] Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». № 48 // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

§ 4. Квалифицирующие признаки состава мошенничества в сфере компьютерной информации

Квалифицирующие признаки состава преступления представляют повышенную общественную опасность, поэтому данный вопрос имеет значительный вес в науке и практике.

В составе мошенничества в сфере компьютерной информации совокупностью законодатель предусматривает наличие отягчающих или квалифицирующих признаков. Итак, в составе ст. 159.6 УК РФ были выделены следующие квалифицирующие признаки:

- деяние по части 1 статьи 159.6 УК РФ, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину (по части 2);

- деяние, предусмотренное частью 1 или частью 2 статьи 159.6 УК РФ, совершенное лицом с использованием своего служебного положения (по пункту «А», части 3);

- деяние, предусмотренное частью 1 или частью 2 статьи 159.6 УК РФ, совершенное в крупном размере (пункт «Б», часть 3);

- деяние, предусмотренное частью 1 или частью 2 статьи 159.6 УК РФ, совершенное с банковского счета, а равно в отношении электронных денежных средств (пункт «В», часть 3);

- деяние, предусмотренное частью 1, частью 2 или частью 3 статьи 159.6 УК РФ, совершенное организованной группой либо в особо крупном размере (по части 4).

Отягчающие признаки рассматриваемого преступления схожи с квалифицирующими признаками других форм хищения.

Стоит начать с рассмотрения такого квалифицирующего признака как «деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину».

Итак, согласно части 2 статьи 35 УК РФ, преступление признается совершенным группой лиц по предварительного сговору, если в нем участвовали

лица, заранее договорившиеся о совместном совершении преступления, при этом, для того, чтобы преступление было признано таковым должно быть установлено не менее двух соисполнителей, а так же взаимная осведомленность и согласованность между ними, единый умысел, кроме того, характер взаимоотношений между соисполнителями должен быть направлен на достижение общего результата – завладение имуществом потерпевшего. Дополнительного, при данном характере отношений, так же важно выполнение каждым соисполнителем своей роли.

Применительно к составу статьи 159.6 УК РФ, групповой характер совершения мошенничества в сфере компьютерной информации может заключаться в осуществлении одним соисполнителем блокировании информации на компьютере, а другим – в любом ином вмешательстве в функционировании информационно-телекоммуникационной сети. А так же, согласно пункту 10 Постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2002 года № 29 «О судебной практике по делам о краже, грабеже, и разбое», «уголовная ответственность за хищение, совершенное группой лиц по предварительному сговору наступает и в тех случаях, когда, согласно предварительной договоренности между соучастниками, непосредственное изъятие имущества осуществляет один из них[1]. И если другие участники в соответствии с распределением ролей совершали согласованные действия, направленные на оказание непосредственного содействия исполнителю в совершении преступления, то содеянное ими является соисполнительством и в силу части 2 статьи 34 УК РФ не требует дополнительной квалификации по статье 33 УК РФ».

Участие в мошенничестве по статьи 159.6 УК РФ лиц, не подлежащих уголовной ответственности в силу возраста или отсутствия вины исключает

[1] Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. – Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

оценку содеянного по признаку совершения преступления группой лиц по предварительному сговору.

Современная правоприменительная практика показывает, что установление признака значительного ущерба зачастую определяется путем сложения сумм денежных средств, полученных в результате совершения лицом ряда тождественных действий по противоправному изъятию имущества.

Кончено же стоит отметить, что данный признак несет за собой оценочный характер, минимальный размер ущерба 2500 рублей (согласно статьи 7.27 КоАП РФ), а максимальный – не должный превышать 250000 рублей.

Так же, согласно пункту 31 Постановлению Пленуму Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» при решении вопроса о наличии в действиях квалифицирующего признака причинение гражданину значительного ущерба судам, наряду со стоимостью похищенного имущества, надлежит учитывать имущественное положение потерпевшего, в частности наличие у него источника доходов, их размер и периодичность поступления, наличие у потерпевшего иждивенцев, совокупный доход членов семьи, с которыми он ведет совместное хозяйство[1]. Мнение потерпевшего о значительности или незначительности ущерба, причиненного ему в результате преступления, должно оцениваться судом в совокупности с материалами дела, подтверждающими стоимость похищенного имущества и имущественное положение потерпевшего.

Так, например, к уголовной ответственности по части 2 статьи 159.6 УК РФ привлечен И. использовавший персональный компьютер, который был подключен к сети «Интернет», с личного электронного счета Р. в системе «Единый кошелек» путем перечисления на счет платежной системы «Киви-кошелек» похитил денежные средства в сумме 5560 рублей 60 копеек, после чего перечислил данную сумму на свой банковский счет в ОАО «Экспресс-банк» и

[1] Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». № 48 // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. – Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

обналичил посредством снятия через банкомат, причинив таким образом ущерб потерпевшему Р.[1].

Так же, Г., будучи осведомлен о механизме перевода денежных средств с банковских карт клиентов ПАО «С.», путем удаленного доступа через сеть «Интернет», с помощью системы дистанционного банковского обслуживания «Банк-онлайн» решил совершить мошенничество в сфере компьютерной информации. Действуя с преступным умыслом, для достижения желаемого преступного результата следующую схему мошенничества в сфере компьютерной информации: в ночное время отыскать в мусорных корзинах, стоящих рядом с банкоматами ПАО «С.», чек-идентификатор и чек с одноразовыми паролями, используя которые путем удаленного доступа через сеть «Интернет» с помощью системы дистанционного банковского обслуживания «Банк-онлайн» незаконно проникнуть в «личный кабинет» клиента ПАО «С.», расположенный на сайте ПАО, для получения возможности распоряжаться денежными средствами, находящимися на счете его банковской карты, после чего с помощью электронных поручений осуществить переводы с этого счета денежных средств на счет имеющейся у него в распоряжении банковской карты. Получив реальную возможность распоряжаться похищенными при указанных выше обстоятельствах денежными средствами, зачисленными на счет имеющейся у него в распоряжении банковской карты, обратить их в свою пользу. Приступив к реализации преступного умысла, направленного на хищение чужого имущества путем ввода компьютерной информации в функционирование средств хранения, обработки и передачи компьютерной информации, Г., под предлогом отсутствия у него банковской карты и необходимостью получения денежных средств, попросил у ранее знакомого К. в пользование принадлежащую последнему банковскому карту. Неосведомленный о преступных намерениях Г. К. согласился и предоставил Г. свою банковскую карту. Продолжая реализовывать преступный умысел Г.

[1] Приговор Каспийского городского суда от 26 июня 2013 года по делу № 1-130/2013 Архив Каспийского городского суда

незаконно получил чек-идентификатор и чек с одноразовыми паролями для входа в систему дистанционного банковского обслуживания «Банк-онлайн». После чего Г., используя ранее незаконно полученные им чек-идентификатор и чек с одноразовыми паролями, путем удаленным доступа через сеть «Интернет» с помощью системы дистанционного банковского обслуживания «Банк-онлайн» незаконно проник в «личный кабинет» Б., находящийся на сайте ПАО «С.», где размещалась информация о денежных средствах, находящихся на счете банковской карты, эмитированной Б. ПАО «С.», и, путем ввода компьютерной информации, осуществил 14 переводов денежных средств на счет банковской карты К., в результате чего Г. получил реальную возможность распоряжаться денежными средствами, похищенными у Б. В результате вышеописанных преступных действий Г. причинил Б. значительный ущерб[1].

Подводя итог, стоит отметить, что:

1) Такой признак как значительный ущерб носит оценочный характер, минимальный размер которого установлен в статье 7.27 КоАП РФ и составляет не более 2500 рублей, а максимальный размер ущерба не должен превышать 250000 рублей. Крупный размер не должен превышать миллиона рублей, а особо крупный превышает миллион рублей;

2) Групповой характер совершения мошенничества в сфере компьютерной информации может заключаться в осуществлении соисполнителями разных функций или способов совершения преступления, например, одним исполнителем – блокирование информации на компьютере, а другим может заключаться в любом ином вмешательстве в функционировании информационно-телекоммуникационной сети;

3) Такой признак, как совершение преступления лицом с использованием своего служебного положения имеет отношение к лицам, приведенным в примечании к статье 285 УК РФ и статье 201 УК РФ;

---

[1] Приговор Промышленного районного суда г. Самара Самарской области от 4 октября 2016 г. по делу № 1-206/2016 Архив Промышленного районного суда г. Самара Самарской области

4) Признак организованной группы в части 4 статьи 159.6 УК РФ вступает в силу, если указанные действия совершенны устойчивой преступной группой лиц, которые заранее объединились и приготовились к совершению одного или нескольких преступлений.

ГЛАВА 2. ОТГРАНИЧЕНИЕ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ОТ СМЕЖНЫХ СОСТАВОВ ПРЕСТУПЛЕНИЙ

§ 1. Проблемы отграничения мошенничества в сфере компьютерной информации от преступлений, предусмотренных ст. ст. 159-159.5

В 2012 году в УК РФ была введена статья 159.6, касающаяся преступлений в сфере компьютерной информации. Ранее, до 2012 года, такие преступления рассматривались в рамках главы 28 УК РФ. Несмотря на то, что уже более восьми лет мошенничество в компьютерной сфере было выделено в отдельный состав и перенесено в другую главу, все еще возникают проблемы с его отличением от других преступлений.

Хотя способы мошенничества в сфере компьютерной информации имеют свои особенности, отличающие их от общей нормы статьи 159 УК РФ, они всё же подчинены основным способам мошенничества - обману и злоупотреблению доверием. Эти способы совершаются в рамках указанных действий, связанных с вводом, удалением, блокированием, модификацией компьютерной информации или вмешательством в функционирование средств хранения, обработки или передачи информации. Поэтому, когда имеются признаки обмана и злоупотребления доверием, такие действия квалифицируются по статье 159.6 УК РФ.

Специалисты различают подходы к интерпретации статей УК РФ о преступлениях в сфере экономики. Например, Т.В. Кленова считает, что законодатель не смог четко определить нормы и установил новые уголовные статьи без необходимости[1]. Её мнение основано на том, что новые нормы неудовлетворительны и не оправдали себя.

Не все теоретики уголовного права поддерживают данную позицию. Например, Л. Гаухман отмечает, что статьи 159.1-159.6 УК РФ следует

[1] Кленова Т.В. О разграничении смежных и конкурирующих составов преступлений (на примере мошенничества) // Уголовное судопроизводство. 2014. № 1. С. 25-30.

рассматривать как привилегированные составы преступлений по сравнению с общей нормой статьи 159.6 УК РФ[1]. Это говорит о том, что есть различные точки зрения на этот вопрос среди специалистов в данной области.

По мнению В.Г. Шумихина, мошенничество в области компьютерной информации не считается специализированным преступлением по отношению к статье 159 Уголовного кодекса РФ. Он основывает свою точку зрения на отсутствии в статье 159.6 УК РФ упоминания о формообразующем признаке мошенничества - способе совершения преступления в виде обмана или злоупотребления доверием, в отличие от других статей (статьи 159.1-159.5 УК РФ). В связи с этим автор делает вывод о том, что объективная сторона статьи 159 и статьи 159.6 УК РФ не совпадает. По его мнению, преступление, предусмотренное статьей 159.6 УК РФ, является самостоятельной формой хищения.

В контексте компьютерной информации, отсутствие указания основных способов мошенничества в норме не является основанием для вывода о их отсутствии в качестве признаков мошенничества. Название нормы подразумевает их существование, что необходимо учитывать.

Некоторые исследователи высказывают мнение о возможных ошибках в разграничении статей 159.6 и 159.3 УК РФ. Например, Е.И. Майорова указывает на проблему различия этих норм, когда виновный, используя компьютерную информацию, совершил хищение денежных средств с чужой платежной карты обманом[2]. Хотя объективная сторона данных преступлений имеет много общего, они не совпадают.

В УК РФ, в статье 159.3, устанавливается, что хищение осуществляется при помощи поддельной или чужой кредитной, расчетной или иной платежной карты, путем обмана работника, уполномоченного кредитной, торговой или другой организацией. Стоит отметить, что основные инструменты,

---

[1] Гаухман Л. Мошенничество: новеллы уголовного законодательства // Уголовное право. 2013. № 3. С. 25-27.

[2] Майорова Е.И. Некоторые проблемы совершенствования уголовного законодательства России на современном этапе // Российский следователь. 2014. № 1. С. 27-31.

используемые для совершения этого преступления, совпадают с теми, которые указаны в статье 159.6 УК РФ - это платежная карта и другие средства хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационные сети. Необходимо отметить, что законодатель включает эти элементы в структуру преступления.

В уголовном законодательстве Российской Федерации применяется понятие "использование", которое охватывает любой способ совершения данного преступления, включая введение компьютерной информации и другие виды вмешательства в работу устройств для хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, предусмотренные в статье 159.3 УК РФ.

Для того чтобы воспользоваться поддельной или чужой кредитной, расчетной или другой платежной картой, необходимо провести манипуляции с работником организации, который обязан решить вопрос.

Подделка или изменение данных при совершении покупок с использованием банковской карты в торговых или сервисных центрах является формой мошенничества в соответствии с постановлением Верховного Суда[1]. Неправомерное использование чьей-то карты или предъявление поддельного паспорта для оплаты товаров не признается мошенничеством по законодательству Российской Федерации, но остается преступлением по другой статье Уголовного кодекса Элемент обмана уполномоченного работника кредитной, торговой или иной организации является не просто обязательным признаком мошенничества, предусмотренного ст. 159.3 УК РФ, а непосредственно сопутствует действиям по изъятию имущества.

Хотя средства и способы совершения преступлений у разных составов могут быть похожими, механизм совершения преступлений и специфика использования средств преступления имеют фундаментальные различия.

---

[1] Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. – Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

Особенности взаимодействия с лицами, попадающими в ловушку обмана или заблуждения, играют решающую роль в этом процессе. Например, при мошенничестве с использованием платежных карт, предусмотренного законом, обман происходит напрямую, когда мошенник обманывает продавца или банковского работника. В отличие от этого, мошенничество в сфере компьютерной информации включает опосредованный обман через онлайн коммуникацию, где преступник использует компьютерную информацию вместо платежной карты.

Подчеркиваем, что ст. 159.3 УК РФ значительно ограничивает разнообразие методов кражи. Мы одобряем заключения, представленные в отчете.

В отличие от мошенничества с использованием платежных карт, преступление в компьютерной сфере допускает совершение как обманом, так и злоупотреблением доверием, в соответствии с статьей 159.3 УК РФ.

Рассмотрев представленный материал, можно заключить, что различие между статьей 159.6 УК РФ и смежными составами осуществляется через специальный подход к совершению преступления, который уникален для мошенничества в сфере компьютерной информации и отличается от способа совершения преступления, описанного в статье 159 УК РФ и статье 159.3 УК РФ. В последнем случае различие также должно быть проведено на основе характера реализации основного способа совершения преступления. Если рассматривать мошенничество с использованием платежных карт, то обман осуществляется лично и напрямую в отношении уполномоченного работника кредитной, торговой или другой организации.

§ 2. Отграничение мошенничества в сфере компьютерной информации от неправомерного доступа к компьютерной информации

На настоящий момент основное отграничение ст. 159.6 УК РФ следует проводить со ст. 272 УК РФ, поскольку именно эти два состава имеют схожие между собой черты. Однако при детальном рассмотрении это абсолютно два

разных состава, разграничивать которые крайне необходимо, поскольку ответственность наступает за совершенно разные деяния.

Рассматриваемый в ч. 1 ст. 159.6 УК РФ основной состав предполагает две составляющие:

1) неправомерное завладение злоумышленником компьютерной информацией - в зависимости от характера преступления ответственность за данные действия наступает согласно ст. 272 либо ст. 273 УК РФ;

2) присвоение чужого имущества путем использования информации, полученной незаконным путем с целью хищения, например, денежных средств с банковской карты, - ответственность должна наступать согласно требованиям ст. 69 УК РФ по совокупности преступлений, в число которых войдет и ст. 159.6 УК РФ.

На приведенном примере можно выявить первые отличия указанных составов: касаемо объекта и предмета посягательства. Дело в том, что в ст. 272 УК РФ предметом посягательства является и информация, содержащаяся в компьютере, и компьютер, который выступает носителем информации, а объектом деяния выступают общественные отношения, обеспечивающие безопасность информации. В случае наличия состава ст. 159.6 УК РФ предметом деяния является чужое имущество или право на него.

Но при этом следует отметить, что безопасность компьютерной информации может выступать дополнительным объектом мошенничества, а хищение собственности - дополнительным объектом неправомерного доступа к компьютерной информации, совершенного с корыстными целями. Так, Куницына Г.С. совершила неправомерный доступ к охраняемой законом компьютерной информации, что повлекло блокирование и уничтожение компьютерной информации при следующих обстоятельствах. Куницина Г.С., обладая знаниями в области компьютерной техники, в корыстных целях использовала доступ к сети Интернет и сим-карту, а также сотовый телефон. В результате совершения противоправных действий в виде подбора пароля к электронному ящику Куницина получила доступ к компьютерной информации,

которая подлежит защите на основании законодательства. После этого она изменила пароль от этого ящика, что привело к воспрепятствованию пользования им его владельцем Потерпевшей №1. Кроме этого, Куницина также удалила всю информацию, находящуюся в данном почтовом ящике, что привело в непригодное для использования состояние указанной информации, тем самым Куницына Г.С. осуществила неправомерный доступ к информации, блокирование и уничтожение информации, содержащейся в электронном почтовом ящике[1].

Обращаясь к разграничению ст. 159.6 и ч. 2 ст. 272 УК РФ, предусматривающей неправомерный доступ к компьютерной информации, совершенный с корыстными целями, можно сказать, что на первый взгляд объективная сторона рассматриваемых составов имеет много сходства. Но стоит учесть, что ввод, удаление, блокирование, модификация или любое иное вмешательство в информацию это лишь способ совершения мошенничества, в то время как, согласно диспозиции ст. 272 УК РФ, названные характеристики являются обязательными последствиями преступления, за которое наступает уголовная ответственность.

Здесь также стоит отметить, что одним из последствий деяния, предусмотренного ст. 272 УК РФ, выступает именно уничтожение информации. Диспозиция же ст. 159.6 УК РФ говорит о том, что мошенничество может быть совершенно путем удаления информации. То есть уже на этом этапе видно различие между составами. Однако, правоприменитель зачастую не разграничивает между собой уничтожение информации и ее удаление, хотя по своей сущности - это абсолютно различные деяния. Уничтожение и удаление рассматриваются судами в каждом из этих случаев, как создание условий, при которых использование информации невозможно.

Так, Первоуральский городской суд Свердловской области рассматривал уголовное дело, в рамках которого происходило обвинение Поспелова И.Д. в том,

---

[1] Кулешова Н. Н., Христофорова Е. И. Особенности квалификации мошенничества в сфере компьютерной информации // Вопросы науки и образования. 2018. № 14 (26). С. 41-46.

что им было совершено несколько эпизодов преступных деяний, предусмотренных ч. 2 ст. 272 и ч.1 ст. 159.6 УК РФ[1]. Как указывает суд в своем приговоре, в процессе рассмотрения дела установлен факт удаления, уничтожения информации, хранящейся на компьютере, что обусловило создание обстановки, при которой использование информации ее обладателем стало невозможно.

Однако уравнивание удаления и уничтожения информации видится необоснованным, особенно учитывая тот факт, что для одной статьи УК РФ удаление – это способ совершения деяния, а для другой уничтожение – это последствие преступного посягательства.

Разграничение стоит проводить и по субъективной стороне: деяние, предусмотренное ст. 159.6 УК РФ, характеризуется прямым умыслом, при этом обязательное условие состоит в том, что виновный руководствуется материальными целями. В отличие от мошенничества в сфере компьютерной информации при неправомерном доступе, согласно ч. 2 ст. 272 УК РФ, для преступника важно получение определенной информации, которая в дальнейшем поможет злоумышленнику получить выгоду имущественного характера, не связанную с незаконным приобретением имущества.

Различие существует и в санкциях. За основной состав мошенничества в сфере компьютерной информации самое строгое наказание не связано с лишением свободы, тогда как за неправомерный доступ размер наказания по ч. 2 ст. 272 УК РФ значительно строже: до четырех лет лишения свободы.

В разъяснениях постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» обращается внимание на то, что мошенничество в сфере компьютерной информации, совершенное путем неправомерного доступа к ней или посредством создания, использования и распространения вредоносных

[1] Приговор № 1-242/2016 Первоуральский городской суд Свердловской области //Архив Первоуральского городского суда Свердловской области

компьютерных программ, требует дополнительной квалификации по ст. 272, 273 или 274.1 УК РФ[1].

Здесь также стоит обратить внимание на то, что если лицо воспользовалось полученной информацией не с корыстными целями, то уголовная ответственность по ст. 159.6 УК РФ не наступает. До введения указанной статьи такое преступление квалифицировалось бы по совокупности с учетом требований ст. 272 (273) и 159 (158) УК РФ.

[1] Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». № 48 // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. – Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

ЗАКЛЮЧЕНИЕ

Анализ проведенного исследования позволяет прийти к следующим выводам:

1. Мошенничество в сфере компьютерной информации является специальным видом мошенничества, которое также посягает на отношения собственности, но при этом совершается специфическими способами. Объектом данного правонарушения выступают отношения, посягающие на право собственности граждан или юридических лиц, дополнительный объект - правоотношения, обеспечивающие информационную безопасность. Объективная же сторона может быть выражена только в активных действиях, как на то указывает законодатель. В вопросе квалификации данного деяния большое значение имеют способы совершения подобного рода посягательства, к которым относятся: ввод, удаление, блокирование, модификация компьютерной информации или иное вмешательство, которое влечет за собой последствия в виде причинения ущерба субъектам права. Наиболее распространённым способом совершения преступления выступает - ввод удаление, блокирование, модификация компьютерной информации, лицами, имеющими доступ к базам данных, а также вмешательство с использованием вредоносных программ.

2. Субъект преступления, предусмотренного ст. 159.6 УК РФ общий. Привлечь к ответственности за совершение мошенничества в сфере компьютерной информации возможно физическое лицо, достигшее возраста шестнадцати лет и отвечающее критериям вменяемости, за исключением п. «а» ч. 3 с. 159.6 УК РФ, поскольку на основании данной нормы субъектом выступает лицо, использующее свое служебное положение в преступных целях. Субъективная сторона преступного посягательства предполагает умышленную форму вину и корыстную цель совершения преступления.

3. Основным преступлением, с которым смешивается мошенничество в сфере компьютерной информации, выступает неправомерный доступ к компьютерной информации. Об этом свидетельствуют и материалы судебной практики. Однако отграничивать данные посягательства между собой крайне

важно – поскольку они имеют различный объект и соответственно различную степень общественной безопасности, что в конечном итоге отражается на применяемой по отношению к виновной санкции.

Кроме того, согласно разъяснениям Пленума ВС РФ действия виновного, должны быть расценены не только по ст. 159.6 УК РФ, но также и по соответствующей норме главы 28 УК РФ.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). – Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 17.06.1996, № 25, ст. 2954. Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

3. Уголовно-исполнительный кодекс Российской Федерации от 08.01.1997 № 1-ФЗ (ред. от 24.06.2023) (с изм. и доп., вступ. в силу с 11.12.2023) Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

4. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 22.04.2024) (с изм. и доп., вступ. в силу с 15.05.2024) Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

5. Гражданский кодекс Российской Федерации (ГК РФ) от 30 ноября 1994 № 51-ФЗ Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

6. Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31 июля 2020 г. № 259-ФЗ Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

II. Учебная, научная литература и иные материалы

1. Барчуков В. К. К вопросу о содержании признаков объективной стороны мошенничества в сфере компьютерной информации // Безопасность бизнеса. – 2016. – № 5. – С. 41–46.

2. Безверхов А. Г. Мошенничество и его виды: вопросы законодательной регламентации и квалификации // Уголовное право. 2015. №5. С. 8 – 14.

3. Гарбатович Д.А. Проблемные аспекты эффективности норм, предусматривающих ответственность за совершение преступлений в сфере компьютерной информации // Библиотека криминалиста. – 2013. – С. 6-14.

4. Гладких В.И. Компьютерное мошенничество: а были ли основания для криминализации? // Рос. следователь. – 2014. – № 22. – С. 25-31.

5. Грунтов И.О. К вопросу о понимании объекта преступления в уголовном праве /И.О. Грунтов // Труд. Работа. Профсоюз. Общество. – 2017. – № 2(56). – С. 41 – 46.

6. Дворецкий М. Ю. Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики // Вестник ТГУ. 2013. №8 (124). С. 407 – 410.

7. Дворецкий М.Ю., Стромов В.Ю. Эффективная реализация уголовной ответственности: проблемы теории и правоприменительной практики // Вестник Московского университета МВД России. 2014.С. 87-94.

8. Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: автореф. дис. ... канд. юрид. наук, М., 2007. – 34 с.

9. Иващенко Н.Д. Мошенничество в сфере компьютерной информации: проблемные вопросы // Столица науки. 2020. № 6. С. 269-276.

10. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия–Телком, 2002. – 336 с.

11. Коростелев М. А. Правовой режим электронных денег в гражданском законодательстве: автореф. дис. . канд. юрид. наук. М., 2015. – 36 с.

12. Кропачев С.Ю. Мошенничество в сфере компьютерной информации как угроза экономической деятельности: актуальные вопросы квалификации // Современная наука: актуальные проблемы теории и практики. серия: экономика и право. 2020. № 4. С. 183 – 187.

13. Кулешова Н. Н., Христофорова Е. И. Особенности квалификации мошенничества в сфере компьютерной информации // Вопросы науки и образования. 2018. № 14 (26). С. 41-46.

14. Курс мировой и российской криминологии в 2 т. Т. II. Особенная часть: учебник для вузов / В. В. Лунеев. - М.: Издательство Юрайт, 2015. - 872 с.

15. Лопатина Т. М. Проблемы уголовно- правовой защиты сфер компьютерной информации: современный взгляд на мошенничество // Право и безопасность. 2013. №3-4 (45). С. 98 – 95.

16. Иногамова-Хегай Л. В. Мошенничество, присвоение, растрата: проблемы квалификации конкурирующих и смежных норм // Уголовное право. 2015. №5. С. 30 – 34.

17. Гаухман Л. Мошенничество: новеллы уголовного законодательства // Уголовное право. 2013. № 3. С. 25-27.

18. Кленова Т.В. О разграничении смежных и конкурирующих составов преступлений (на примере мошенничества) // Уголовное судопроизводство. 2014. № 1. С. 25-30.

19. Майорова Е.И. Некоторые проблемы совершенствования уголовного законодательства России на современном этапе // Российский следователь. 2014. № 1. С. 27-31.

III. Эмпирические материалы

1. Статистика и аналитика.−URL: http://www.mvd.ru. (дата обращения: 10.04.2024).

2. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». № 48 // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. – Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

3. Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» // КонсультантПлюс:

справ. правовая система. Версия Проф. М., 2020. – Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru

4. Приговор № 1-242/2016 Первоуральский городской суд Свердловской области //Архив Первоуральского городского суда Свердловской области

5. Приговор Промышленного районного суда г. Самара Самарской области от 4 октября 2016 г. по делу № 1-206/2016 Архив Промышленного районного суда г. Самара Самарской области

6. Приговор Каспийского городского суда от 26 июня 2013 года по делу № 1-130/2013 Архив Каспийского городского суда

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну. А.Н. Черепанов