Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение
высшего образования «Казанский юридический институт
Министерства внутренних дел Российской федерации»

Кафедра уголовного права

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему: Актуальные вопросы квалификации кражи и мошенничества, совершаемые с использованием компьютерной информации

Выполнил: Якупов Равиль Рамилевич,
40.05.01 – Правовое обеспечение национальной безопасности, 2012 года набора, группа № 123

Руководитель:
_____
_____
_____

Консультант:
_____
_____
_____

Рецензент:
_____
_____
_____

К защите:_____
(допущена, не допущена)

Начальник кафедры
_____Р.С. Куликов

Дата защиты: «__» _____2017 г. Оценка _____

Казань 2017

Содержание

ВВЕДЕНИЕ 3
ГЛАВА I. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ 8
§1. Объективные признаки состава преступления 8
§2. Субъективные признаки состава преступления 20
§3. Квалифицирующие признаки состава преступления 28
ГЛАВА II. ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, ПРЕДУСМОТРЕННЫХ СТАТЬЕЙ 159.6 УК РФ И ОТГРАНИЧЕНИЕ ЕГО ОТ СМЕЖНЫХ СОСТАВОВ 35
§1. Отграничение мошенничества с использованием компьютерной информации от смежных составов преступления 35
§2. Актуальные проблемы противодействия мошенничества в сфере компьютерной информации уголовно-правовыми средствами и пути их преодоления 46
ЗАКЛЮЧЕНИЕ 60
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ 64

Введение

Компьютерное мошенничество (computer fraud) получило свою популярность в 1970-е годы (время распространения компьютерных технологий и внедрения их в различные сферы жизнедеятельности). Преступники начали активно использовать возможности новых технологий для взлома баз данных, в том числе банков и правительств. В связи с этим ряд государств дополняют свое уголовное законодательство нормами об ответственности за мошенничество, совершенное с помощью компьютерной информации и информационных технологий. Так, в Уголовном кодексе Германии появился § 263а, предусматривающий ответственность за причинение имущественного ущерба путем воздействия на результат обработки данных с помощью специальных программ, использования неправильных или неполных данных, неправомочного использования данных или иного воздействия на результат обработки данных[1] . В санкции статьи, предусматривающей ответственность за мошенничество по Уголовному кодексу Швеции, присутствует указание на способ совершения преступления с помощью компьютерных технологий: "За мошенничество должно быть привлечено к ответственности лицо, которое, используя ложную или неполную информацию, изменяя программы, или любыми другими средствами незаконно вмешивается в процессы автоматической обработки данных, другие автоматические процессы, извлекает выгоду для себя, причинив при этом ущерб имуществу собственника"[2]. В 1987 году австрийское правительство дополнило Уголовный кодекс ст. 148а об

---

[1] Уголовный кодекс Федеративной Республики Германия от 15.05.1871 (в ред. от 13 ноября 1998 г.). Особенная часть. СПб.: Юридический центр "Пресс", 2003. С. 203.

[2] Уголовный кодекс Швеции от 01.01.1962 / Под ред. С.С. Беляева, Н.Ф. Кузнецовой. СПб.: Юридический центр "Пресс", 2001. С. 154.

ответственности за имущественный вред, причиненный с целью извлечения незаконной выгоды для преступника или третьего лица, путем влияния на процессы автоматизированной обработки данных с помощью специальных программ, ввода, изменения или уничтожения данных или иным способом, влияющим на процесс обработки данных[1].

Актуальность данной темы обусловлена тем, что с момента дополнения Уголовного кодекса РФ шестью новыми составами, предусматривающими ответственность за различные виды мошенничества, число преступных посягательств на имущество, совершаемых путем обмана или злоупотребления доверием, продолжает расти. Так, в 2015 году в России зарегистрировано 196700 преступлений, ответственность за которые предусмотрена статьями 159 - 159.6 УК РФ (на 25% больше аналогичного периода 2014 года - 160214). На фоне общего роста числа зарегистрированных мошенничеств наблюдается значительный рост так называемых компьютерных мошенничеств, который составил 447% (с 995 по итогам 2014 года до 5443 в 2015 году). При этом раскрываемость последних по итогам 2015 года находилась на низком уровне и составляла лишь 7,4% (в 2014 году - 32,2%). По итогам 4 месяцев 2016 года негативная тенденция сохранилась: в России зарегистрировано 1789 компьютерных мошенничеств (+143,7%). Лидируют по числу данных преступлений Тюменская область (333 факта), Удмуртская Республика (298), Республика Коми (223). Раскрыто всего 72 преступления (-5,3% по сравнению с аналогичным периодом 2015 года). Существенное снижение числа раскрытых преступлений обусловлено совершенствованием способов посягательств, которым на данный момент органы внутренних дел не готовы противостоять[2].

---

[1] Уголовный кодекс Австрии от 29.01.1974. СПб.: Юридический центр "Пресс", 2004. С. 172.

[2] Информация Центра статистической информации Главного информационно-аналитического центра МВД России.

Все это указывает на то, что в современном преступном мире все больше внимания уделяется на преступления, совершаемые посредством компьютерных технологий. Для борьбы с новыми видами преступлений исполнительными и законодательными органами власти создаются и реализуются новые механизмы противодействия компьютерным преступлениям.

Степень научной разработанности проблемы исследования. Отдельным проблемам уголовно-правовой охраны собственности от мошеннических посягательств с использованием компьютерной информации в отечественной юридической литературе уделялось внимание. Вопросы мошенничества в сфере Интернет и компьютерной информации рассматривали Д.А. Зыков, Т.М. Исаева, Т.П. Кесарева, С.П. Кушпиренко, А.JI. Осипенко, А.Е. Шарков и др. Рассмотрением вопросов мошенничества в сетях сотовой связи занимались Н.П. Бирюков, Г.В. Семенов, З.А. Ибрагимова, И.В. Лазарева и др. Различные аспекты уголовно - правового анализа мошенничества в сфере безналичной оплаты затрагивались в трудах Д.Р. Алембекова, А.Ю. Афанасьева, С.С. Карабанова, А.А. Пальянова, В.П. Трухина, А.В. Шмонина и др.

Мы считаем, что необходим комплексный уголовно-правовой анализ мошенничества в сфере компьютерной информации, что требует более конкретного теоретического осмысления. Это обуславливается постоянным изменением и усложнением способов совершения мошеннических действий с использованием компьютерной информации.

Цели и задачи исследования. Основной целью исследования является рассмотрение в уголовно-правовом поле мошенничества с использованием компьютерной информации и ограничение интернет-мошенничества от смежных ему составов преступления.

Для достижения указанной цели сформулированы следующие основные задачи:

1. Изучить и провести анализ признаков состава преступления, предусмотренного статьей 159.6 Уголовного Кодекса РФ (мошенничество в сфере компьютерной информации)

2. Рассмотреть научные концепции понятий «уголовно-правовая характеристика преступления», «компьютерная информация», «информация», практическая реализация которых в значительной мере определяет квалификацию преступлений.

3. Разработать методические рекомендации, направленные на повышение эффективности разграничения и расследования мошенничества в сфере компьютерной информации от смежных составов.

Объект и предмет исследования. Объектом исследования являются общественные отношения, возникающие в сфере уголовно-правового противодействия мошенничеству с использованием компьютерной информации, а также разграничение указанного вида преступления от смежных.

Предметом исследования являются уголовно-правовые нормы, устанавливающие ответственность за мошенничество в сфере высоких технологий и компьютерной информации с применением глобальной сети Интернет.

Методология и методика исследования. При проведении исследования, исходя из особенностей его объекта, предмета, целей и задач, использовалась следующая методологическая основа: диалектический метод познания явлений и процессов социальной реальности, рассматривающий их в постоянном изменении, развитии, и частно-научные методы: системно-структурный, логический, сравнительного правоведения, метод экспертных оценок, а также статистический метод исследования.

Научная новизна исследования. В работе представлен уголовно-правовой анализ состава преступления, а именно мошенничества с использованием компьютерной информации. В исследовании отражаются дискуссионные вопросы отграничения преступления (мошенничества с

использованием компьютерной информации) от смежных ему составов преступления, затрагиваются вопросы ответственности и наказания, а также вносятся предложения по совершенствованию действующего уголовного законодательства в сфере преступлений, связанных с компьютерной информацией.

ГЛАВА 1. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§1. Объективные признаки состава преступления

В ст. 35 Конституции РФ закреплено: право частной собственности охраняется законом (ч. 1); каждый вправе иметь имущество в собственности, владеть, пользоваться и распоряжаться им как единолично, так и совместно с другими лицами (ч. 2). Часть 1 ст. 209 Гражданского кодекса РФ раскрывает содержание правомочий собственника: "Собственнику принадлежат права владения, пользования и распоряжения своим имуществом".

Значимость права собственности диктует особые меры охраны, в том числе и с помощью уголовно-правовых норм. Как отмечает Е.А. Суханов, правовое регулирование отношений собственности складывается из правил (норм) поведения, в которых устанавливается сама возможность (или невозможность) принадлежности материальных благ определенным лицам (или коллективам), определяются пределы их правомочий, а также правовые способы защиты от посягательств на охраняемые возможности хозяйственного господства над имуществом[1]. Статьи главы 21 Уголовного кодекса[2] РФ направлены на защиту прав собственников и иных владельцев имущества и предусматривают меры уголовной ответственности за преступления в данной сфере. Однако нельзя сказать, что уголовно-правовая охрана собственности осуществляется на должном уровне.

---

[1] Суханов Е.А. Лекции о праве собственности. М., 1991. С. 16.

[2] Далее – УК.

Опасность хищений состоит в их особой значимости для повседневной жизни субъектов сложившихся правоотношений. По справедливому замечанию Г.Н. Борзенкова, общественная опасность хищений чужого имущества (основная группа преступлений против собственности) определяется еще и тем, что в своей массе они вносят дезорганизацию в экономическую жизнь страны, создают возможности для паразитического обогащения одних за счет других, негативно влияют на неустойчивых членов общества[1]. Разрушение соответствующих отношений собственности вследствие преступных посягательств имеет серьезные негативные последствия. Собственникам причиняется имущественный, а порой и физический вред. В определенных сферах такой ущерб весьма существенный, который отражается на материальном благополучии, на экономических возможностях потерпевших. Страдает и вся нравственная оболочка, которая позволяет говорить о свободном человеке - обладателе того или иного имущества.

Особое место среди хищений занимают деяния, совершаемые путем обмана или злоупотребления доверием (мошенничество), которые весьма распространены и обладают высокой латентностью.

Мошенничество в сфере компьютерной информации (159.6 УК РФ) была введена в Уголовный кодекс РФ 29 ноября 2012 года Федеральным законом от № 207-ФЗ. Новая разновидность мошенничества предполагает совершение 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.

Исходя из содержания пояснительной записки к законопроекту о внесении данных изменений, их целью являлась дифференциация различных

[1] Курс уголовного права: В 5 т. Общая часть / Под ред. Н.Ф. Кузнецовой, И.М. Тяжковой. Особенная часть / Под ред. Г.Н. Борзенкова и В.С. Комиссарова. М.: Зерцало-М, 2002.

видов мошенничества, специализированных сферой экономической деятельности, в которой они совершаются, и способом совершения преступления, а также особым предметом посягательства. В рассматриваемом случае критерием дифференциации выступил способ совершения преступления[1].

В рамках настоящего исследования необходимо изучить понятие объекта и их классификацию, т.к. объект, его вид и характер непосредственно влияют на свойство тех признаков, что следует назвать в настоящей работе и непосредственно изучить.

Включение мошенничества в сфере компьютерной информации в состав главы 21 УК РФ предусматривает в качестве видового объекта отношения собственности, непосредственным объектом выступает чужое имущество или права на него.

В науке уголовного права общепризнано, что видовым объектом хищений признаются общественные отношения, обеспечивающие осуществление собственником или иным лицом законного права на владение, пользование и распоряжение имуществом. Мы поддерживаем такое определение, но считаем, что более развернутое определение видового объекта дано авторами Курса российского уголовного права: "Видовым объектом преступлений против собственности являются отношения собственности в сфере производства, потребления и распределения материальных благ, включающих права собственника по владению, пользованию и распоряжению своим имуществом, а также права лица, хотя и не являющегося собственником, но владеющего имуществом на праве

[1] Пояснительная записка к проекту Федерального Закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» (в части дифференциации мошенничества на отдельные составы) // СПС Консультант Плюс.

хозяйственного ведения, оперативного управления либо по иному основанию, предусмотренному законом или иным правовым актом"[1].

Наряду с родовым и видовым объектом для уяснения состава преступления важное значение имеет непосредственный объект. По мнению Г.П. Новоселова, в реальной действительности нет никакого иного объекта, кроме того, который сторонники квалификации объектов преступления "по вертикали" называют непосредственным. Под ним понимается вид общественных отношений, на которые посягает одно или несколько преступлений. Можно уточнить в этой части, что речь идет о конкретном отношении, которое подвергается преступному воздействию в реальной ситуации.

Основной объект и предмет рассматриваемого состава преступления, мошенничества в сфере компьютерной информации, не имеют своей специфики и полностью совпадают с общим составом мошенничества, предусмотренного ст.159 УК РФ, то есть это общественные отношения, складывающиеся в сфере распределения и перераспределения материальных благ. Как и мошенничество вообще, квалифицированное мошенничество в сфере компьютерных технологий – всегда хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Согласно ст. 159.6 УК РФ мошенничество в сфере компьютерной информации - это 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. Здесь законодатель упомянул лишь объективные признаки мошенничества в сфере компьютерной информации, среди которых в первую очередь определен предмет

[1] Курс российского уголовного права. Особенная часть / Под ред. В.Н. Кудрявцева, А.В. Наумова. М.: Спарк, 2002. С. 314.

преступления. Так, в отличие от других специальных видов мошенничества (ст. ст. 159.1 - 159.5 УК РФ) предметом преступления, предусмотренного ст. 159.6 УК РФ, может выступать не только имущество, но и право на него. Аналогичный подход к определению предмета преступления имеет место в общем составе мошенничества (ст. 159 УК РФ). Однако, как в общей норме о мошенничестве, так и в специальной (ст. 159.6 УК РФ) уяснение содержания права на имущество сопряжено с определенными сложностями.

Упоминание о праве на имущество содержится в п. 4 Постановления Пленума Верховного Суда РФ от 27 декабря 2007 г. N 51 "О судебной практике по делам о мошенничестве, присвоении и растрате". В частности, в Постановлении указывается, что право на имущество возникает с момента регистрации права собственности на недвижимость или иных прав на имущество, подлежащих такой регистрации в соответствии с законом; со времени заключения договора; с момента совершения передаточной надписи (индоссамента) на векселе и т.д.

Поскольку для данного вида мошенничества специфичен способ совершения преступления, то высказываются мнения, что в этом составе дополнительным объектом могут выступать общественные отношения в сфере защиты компьютерной информации. Данный вывод предполагает, что при квалификации содеянного по ст. 159.6 УК РФ не требуется дополнительной квалификации по преступлениям, посягающих на сферу компьютерной информации.

Однако такой подход следует поставить под сомнение. Посягательство на дополнительный объект должно повышать общественную опасность преступления, находящую свое отражение в более строгой санкции статьи. В то же время санкция специального состава мошенничества, предусмотренного ст.159.6 УК РФ, содержит менее строгое наказание, чем санкции общего состава мошенничества (ч.1 ст.159 УК РФ), и преступлений в сфере компьютерной информации (ст.ст. 272, 273 УК РФ).

Также остаются в силе разъяснения, данные в постановлении Пленума Верховного Суда РФ от 27.12.2007 N 51 "О судебной практике по делам о мошенничестве, присвоении и растрате". В них указывается, что в случаях, когда мошенничество сопряжено с неправомерным внедрением в чужую информационную систему или с иным неправомерным доступом к охраняемой законом компьютерной информации кредитных учреждений либо с созданием заведомо вредоносных программ для электронно-вычислительных машин, внесением изменений в существующие программы, использованием или распространением вредоносных программ для ЭВМ, содеянное подлежит квалификации по статье 159 УК РФ, а также, в зависимости от обстоятельств дела, по статьям 272 или 273 УК РФ, если в результате неправомерного доступа к компьютерной информации произошло уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.[1]

Особенности объективной стороны мошенничества описаны многими авторами[2]. Более точно нам видится позиция доктора юридических наук, профессора Н.Г. Кадникова, который полагает, что "объективная сторона преступления есть совокупность установленных уголовным законом, а в отдельных случаях (когда диспозиция статьи Особенной части УК РФ является бланкетной) - другими законами или нормативными правовыми актами признаков, характеризующих внешние проявления общественно опасного и противоправного поведения человека, причиняющего

---

[1] Постановление Пленума Верховного Суда РФ от 27.12.2007 N 51 "О судебной практике по делам о мошенничестве, присвоении и растрате"//Бюллетень Верховного Суда РФ, N 2, февраль, 2008.

[2] Кудрявцев В.Н. Объективная сторона преступления. М.: Госюриздат, 1960; Курс советского уголовного права: В 6 т. Часть общая. Т. 2. Преступление. М.: Наука, 1970; Уголовное право России. Общая часть. Особенная часть: Учебник по специальностям "Правоохранительная деятельность", "Правовое обеспечение национальной безопасности" / Под общ. ред. д.ю.н., проф. Н.Г. Кадникова. М.: ИД "Юриспруденция", 2013 и др.

существенный вред объекту уголовно-правовой охраны либо способного причинить такой вред, находящегося в психофизическом единстве с внутренними процессами, отражающими сознание и волю лица, его потребности и интересы, цели и мотивы поведения".

Объективная сторона рассматриваемого вида мошенничества представлена как хищение чужого имущества, то есть противоправное безвозмездное изъятие с корыстной целью и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или иному владельцу этого 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.

Под компьютерной информацией, согласно примечанию к ст.272 УК РФ, понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Особенность мошенничества состоит в способах завладения чужим имуществом. Способы являются в данном случае обязательными признаками объективной стороны и в конечном итоге определяют суть мошенничества. Как отмечается в специальной литературе, проблема способа совершения преступления относится к наименее разработанным в общем учении о преступлении. Относительно понятия способа совершения мошенничества среди криминалистов единое мнение отсутствует. Одни авторы под способами мошенничества понимают многочисленные приемы его совершения, основывая свою позицию на толковом словаре С.И. Ожегова, в котором способ определяется как прием, действие, метод, применяемый при исполнении какой-либо работы, при осуществлении какой-нибудь

деятельности[1]. Другие авторы под способом совершения мошенничества понимают образ действия, определенную последовательность действий[2]. На основе изучения мнений ученых и обобщения материалов судебно-следственной практики Р.Б. Осокин формулирует обоснованный вывод о том, что под способом совершения мошенничества следует понимать определенную последовательность и образ действий, проявляющихся в приемах, методах, совокупности средств, используемых для совершения общественно опасного деяния[3]. В отличие от преступлений, которым присущ физический (операционный) способ, при мошенничестве способ действий преступника носит информационный характер либо строится на особых доверительных отношениях, сложившихся между виновным и потерпевшим. Более точно, на наш взгляд, к определению данного понятия подошла М.В. Шкеле, которая полагает, что способ совершения преступления является одним из признаков объективной стороны каждого преступления, представляет собой форму проявления вовне общественно опасного деяния (действия или бездействия) и раскрывается через систему актов осознанного и волевого поведения, которые могут быть представлены как положительными признаками (совершение определенных активных действий - приемов), так и отрицательными признаками (отсутствие определенных активных действий, которые лицо должно было и могло совершить с учетом конкретных обстоятельств происшедшего) <5>. Как отмечает М.И. Еникеев, способ совершения преступления - это система приемов действий общенациональных комплексов, обусловленных целью и мотивами действия, психическими и физическими особенностями действующего лица, в котором проявляются психофизиологические и характерологические особенности человека, его знания, умения, навыки, привычки и отношение к различным

---

[1] Ожегов С.И. Словарь русского языка. М., 1972. С. 158.

[2] Кудрявцев В.Н. Объективная сторона преступления. М., 1960. С. 11

[3] Осокин Р.Б. Уголовно-правовая характеристика способов совершения мошенничества: Дис. ... канд. юрид. наук. М., 2004. С. 62.

сторонам действительности. Для каждого преступления существует свой системный "набор", комплекс действий и операций. У каждого человека также имеется система обобщенных способов действий, свидетельствующих о его индивидуальных особенностях. Эти комплексы так же индивидуализированы, как и папиллярные узоры пальцев, однако в отличие от последних следы этого комплекса всегда остаются на месте преступления.

Ввод компьютерной информации представляет собой размещение сведений в устройствах ЭВМ для их последующей обработки и (или) хранения. Под удалением компьютерной информации понимается совершение действий, в результате которых становится невозможным восстановить содержание компьютерной информации, и (или) в результате которых уничтожаются носители компьютерной информации.

Блокирование компьютерной информации представляет собой действия, приводящие к ограничению или закрытию доступа к компьютерной информации и характеризующиеся недоступностью ее использования по прямому назначению со стороны законного владельца (собственника). Оно осуществляется путем совершения действий по изменению или установлению пароля, логина, в результате чего происходит ограничение (закрытие) доступа к информационным ресурсам. Моментом окончания этого действия выступает отсутствие доступа к компьютерной информации в определенный промежуток времени или постоянно. Все другие действия, которые могут быть на практике совершены, находятся за рамками состава преступления. Поэтому ущерб определяется размером выгоды, полученной только в результате совершения действий по блокированию. Однако он выражается не в виде прямого реального ущерба, а в виде упущенной выгоды.

Модификация компьютерной информации осуществляется путем внесения любых изменений сведений (сообщений, данных), представленных в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Модификация компьютерной информации при совершении мошенничества осуществляется путем действий по изменению номера sim-карты, записи на лицевом счете, персональных данных потерпевшего, цены товара, внесения изменений в программу и других действий, результатом которых являются видоизмененные данные на лицевом счете виновного лица, сведения о sim-карте и т.д.

Например, Б., являясь работником банка, имея доступ к компьютерным системам банка, находясь в офисе и используя рабочий компьютер, ввел свой логин и пароль, дающие ему возможность войти в систему "Online", т.е. в компьютерную программу, позволяющую изменять данные и значения расчетных счетов; произвел изменения по своему расчетному счету, увеличив значение доступного остатка на счете с 0 на 6 379 363 руб. С этого момента Б. получил реальную возможность пользоваться и распоряжаться ими по своему усмотрению[1].

Вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или в информационно-телекоммуникационные сети как способ мошенничества представлено в законе в виде действий по вводу, удалению, блокированию, модификации компьютерной информации и действий иного воздействия.

Иное вмешательство (воздействие) отличается от способов, непосредственно выделенных в ст. 159.6 УК РФ, тем, что лицо осуществляет неправомерный доступ к компьютерной информации с использованием незаконно полученных индивидуально учетных данных (пароля, логина и др.) для воздействия на компьютерную информацию способами, рассмотренными выше. Способы получения учетных данных (пароля, логина и др.) могут быть различными (обман потерпевшего, тайное или открытое копирование и др.).

---

[1] Приговор Хорошевского районного суда г. Москвы от 28 ноября 2014 г. по уголовному делу N 1-585/14 // http://судебныерешения.рф/bsr/case/6993929.

Большинство криминалистов полагает, что данный состав является специальным по отношению к общему составу мошенничества, предусмотренному ст.159 УК РФ. Мошенничество отличает от других видов хищения чужого имущества способ его совершения – обман или злоупотребление доверием. Соответственно обман или злоупотребление доверием должны являться конструктивными признаками рассматриваемого нами специального вида мошенничества. Однако данный вывод следует поставить под сомнение по следующим причинам.

В пояснительной записке к проекту Федерального Закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» (в части дифференциации мошенничества на отдельные составы) Верховным Судом, инициировавшим данные изменения, указывалось, что подобные преступления совершаются не путем обмана или злоупотребления доверием конкретного субъекта, а путем получения доступа к компьютерной системе и совершения вышеуказанных действий, которые в результате приводят к хищению чужого имущества или приобретению права на чужое имущество.

Мошенничество относится к преступлениям с материальным составом, и поэтому ущерб, который причиняется собственнику, как обязательный признак объективной стороны характеризует преступные последствия. Эти последствия носят имущественный характер и могут быть оценены в денежном эквиваленте, что в конечном итоге окажет существенное влияние на квалификацию хищения в зависимости от размера похищенного. Важно определить стоимость похищенного. Если это движимая вещь (не являющаяся антиквариатом либо произведением искусства и т.п.), то трудностей, как правило, не возникает. Стоимость похищенного определяется на момент совершения мошенничества. Об этом же указано в разъяснениях Пленума Верховного Суда РФ: "Определяя стоимость имущества, похищенного в результате мошенничества, присвоения или растраты, следует исходить из его фактической стоимости на момент

совершения преступления. При отсутствии сведений о цене похищенного имущества его стоимость может быть установлена на основании заключения экспертов"[1].

Также, на что хотелось бы обратить внимание, - момент окончания мошенничества. В общем составе мошенничества, когда речь идет о хищении имущества, преступление считается оконченным, когда виновный получает реальную возможность распорядиться имуществом по своему усмотрению. В дополнение к этому Пленум Верховного Суда РФ разъяснил, что мошенничество признается оконченным с момента, когда указанное имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность (в зависимости от потребительских свойств этого имущества) пользоваться или распоряжаться им по своему усмотрению[2].

Если мошенничество совершено в форме приобретения права на чужое имущество, преступление считается оконченным с момента возникновения у виновного юридически закрепленной возможности вступить во владение или распорядиться чужим имуществом как своим собственным.

При мошенничестве, совершенном путем перевода безналичных денежных средств, преступление следует считать оконченным с момента зачисления этих средств на счет лица, которое путем обмана или злоупотребления доверием изъяло денежные средства со счета их владельца, либо на счета других лиц, на которые похищенные средства поступили в результате преступных действий виновного.

Сам по себе факт ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или

---

[1] Постановление Пленума Верховного Суда Российской Федерации N 51 от 27 декабря 2007 г. "О судебной практике по делам о мошенничестве, присвоении и растрате"

[2] пункт 4 Постановления Пленума Верховного Суда Российской Федерации N 51 от 27 декабря 2007 г. "О судебной практике по делам о мошенничестве, присвоении и растрате".

информационно-телекоммуникационных сетей в зависимости от обстоятельств дела может содержать признаки приготовления к мошенничеству в сфере компьютерной информации или покушения на совершение такого преступления.

Несмотря на то, что теоретики уголовного права склонны считать новый состав преступления, предусмотренный ст. 159.6 УК РФ, производным от общего состава мошенничества, судебная практика восприняла его как самостоятельную, новую форму хищения чужого имущества, отличающуюся от иных специфичным способом его совершения. Об этом свидетельствует то, что обман и злоупотребление доверием, являясь обязательными признаками любого вида мошенничества, в анализируемом составе таковыми не являются.

§2. Субъективные признаки состава преступления

Поведение человека, в том числе и противоправное, представляет органическое единство внешней (физической) и внутренней (психической) сторон. Поэтому характеристика преступления является неполной без раскрытия признаков субъективной стороны, которые наравне с объективными признаками, должны быть тщательно исследованы и проанализированы правоприменительным органом.

Субъективные признаки состава преступления играют важную роль в оценке противоправного деяния и человека, его совершившего. Очень сложно узнать внутреннюю мотивацию человека, который решился на совершение преступления, раскрыть интеллектуальный и волевой моменты его поведения, чтобы определить форму вины, мотивы и цели, психическое

состояние субъекта и его отношение к наступившим последствиям. Очень мало лиц, преступивших закон, чистосердечно рассказывают о мотивах, внутренних побуждениях и целях, к которым они стремились в момент совершения преступления. В этом же контексте признаки самого субъекта играют определяющую роль. Его психическое состояние, возраст - вот те составляющие, которые частично определены в уголовном законе, частично разъясняются в постановлениях высших судебных органов, а в ряде случаев зависят от опыта, знаний практических работников.

Более правильно анализ начать с субъекта преступления как физического лица, обладающего необходимыми признаками, т.к. признаки субъективной стороны не существуют сами по себе, а только применительно к конкретному физическому лицу.

В общем учении о преступлении субъект - один из признаков состава. Отсутствие в законе этого признака исключает уголовную ответственность[1]. В юридической литературе исследованию понятия субъекта преступления, его общих и специальных признаков уделено заметное внимание. Этой проблеме посвятили свои работы Ю.М. Антонян, С.В. Бородин, П.С. Дагель, Б.А. Куринов, Р.И. Михеев, В.С. Орлов, Ш.С. Рашковская, С.А. Семенов, В.В. Устименко и ряд других авторов.

В реальной жизни субъект преступления - это человек, обладающий не только самыми общими необходимыми для возложения уголовной ответственности признаками (возраст, вменяемость), но и другими качествами, которые могут иметь определенное уголовно-правовое значение. Таковыми могут быть биологические и социальные признаки: пол, состояние здоровья, родственные отношения с потерпевшим, должностное положение, гражданство и иные данные, характеризующие статус человека в обществе. В этой связи, как известно, наряду с понятием "субъект преступления" в уголовном праве используется понятие "личность преступника". Оно

---

[1] Орлов В.С. Субъект преступления по советскому уголовному праву. М., 1958. С. 29.

характеризует участника уголовно-правовых отношений (лицо, совершившее преступление) более основательно, всесторонне включает не только типичные, но и индивидуальные признаки человека, виновного в нарушении уголовно-правового запрета. Таким образом, если признаки субъекта преступления используются именно для ответа на вопрос, имеется ли в данном случае конкретный состав преступления, то признаки, характеризующие личность преступника, имеют существенное значение для индивидуализации уголовной ответственности и назначения наказания.

В УК РФ юридические признаки субъекта определены в ст. 19 - 21, где указывается, что субъектом преступления может быть физическое лицо (человек), вменяемое и достигшее установленного законом возраста. Доктрина российского уголовного законодательства базируется на принципах индивидуальной ответственности физического лица.

За мошенничество ответственность предусмотрена с 16 лет, что позволяет говорить об особом положении субъекта данной формы хищения в сравнении с субъектами по другим формам хищений.

Еще один важнейший признак субъекта преступления - вменяемость. Вменяемость как другой важный признак субъекта преступления является предпосылкой вины и уголовной ответственности, так как лицо, способное сознавать фактический и юридический характер своего поведения и руководить им, может нести уголовную ответственность[1].

Уголовный закон (ст. 21 УК) приводит понятие и условия невменяемости: не подлежит уголовной ответственности лицо, которое во время совершения общественно опасного деяния находилось в состоянии невменяемости, то есть не могло осознавать фактический характер и общественную опасность своих действий (бездействия) либо руководить ими

[1] Уголовное право России. Общая часть. Особенная часть: Учебник по специальностям "Правоохранительная деятельность", "Правовое обеспечение национальной безопасности"/ Под общ. ред. д.ю.н., проф. Н.Г. Кадникова. М.: ИД "Юриспруденция", 2013. С. 143

вследствие хронического расстройства, слабоумия или иного болезненного состояния психики[1]. Признание лица невменяемым предполагает отсутствие состава преступления, но не самого общественно опасного деяния. Орган дознания, следователь составляют вместо обвинительного заключения постановление о направлении дела в суд для применения принудительных мер медицинского характера (ст. 439 УПК). Суд обязан подробно рассмотреть обстоятельства совершения общественно опасного деяния и вынести не приговор, а определение об освобождении от уголовной ответственности и о применении принудительных мер медицинского характера (ст. 443 УПК).

Представляет особый интерес изучение личности мошенника, поскольку это является важной и необходимой предпосылкой профилактики преступного поведения.

Наука уголовного права рассматривает личность преступника в единстве ее социальных, психических и физических особенностей, имеющих уголовно-правовое значение для определения возможности уголовной ответственности и ее индивидуализации, т.е. для определения наличия преступления и его правовых последствий.

Изучение уголовных дел показывает, что чаще всего мошенничество в сфере компьютерной информации совершают лица от 20 до 45 лет. Мошенникам присущ более высокий уровень интеллекта. Среди мошенников около 15% имеют высшее, а около 20% - среднее профессиональное образование. В большинстве случаев привлекаемые к ответственности лица ранее не судимы. Пол - в основном, мужской, но наблюдается тенденция к увеличению числа лиц женского пола. Происходят из семей со средним и выше среднего достатком. При совершении преступлений используют набор заранее подготовленных «инструментов», в основном, готовые решения, разработанные 1-ой группой или другими людьми своей группы, либо

[1] Курс советского уголовного права. Общая часть. М., 1982. Т. 1. С. 231.

являются организаторами хакерских атак с исполнителями из 1-ой группы. Так же нередко идут на совершение преступлений «контактным» способом, часто сопряжённым с насильственными действиями (получение доступа к компьютерной информации с того же компьютера, на котором она размещается, при невозможности удалённого доступа). Мошенникам присущ мощный комбинаторный интеллект, позволяющий строить модели поведения людей под влиянием внешних воздействий, прогнозировать их поведение и предусматривать меры для осуществления мошеннических замыслов.

Очень важным, а порой и определяющим всю дальнейшую ситуацию является такой элемент состава преступления, как субъективная сторона, под которой доктрина уголовного права понимает внутреннюю часть преступного деяния, а именно психическую деятельность субъекта преступления, совершающего общественно опасное действие и причиняющего негативные последствия охраняемым интересам.

Сторона называется субъективной именно потому, что признаки воли и сознания можно наблюдать только у определенного субъекта, человека, наделенного разумом[1]. По весьма точному определению В.Н. Кудрявцева, субъективная сторона преступления представляет собой своеобразную "модель" объективной стороны в психике субъекта. Она включает интеллектуальное и волевое отношение лица к совершаемому им деянию и его последствиям (вина), цели и мотивы его деятельности, а также эмоциональное состояние, характеризующее его психику в момент совершения преступления. Важность и значение точного установления субъективной стороны состава преступления подчеркиваются положениями Конституции РФ (ч. 1 ст. 49), ст. 5 УК РФ, неоднократным обращением на это внимания в постановлениях Пленума Верховного Суда РФ и т.д.

---

[1] Уголовное право России. Общая часть. Особенная часть: Учебник по специальностям "Правоохранительная деятельность", "Правовое обеспечение национальной безопасности"/ Под общ. ред. д.ю.н., проф. Н.Г. Кадникова. М.: ИД "Юриспруденция", 2013. С. 126.

Главным и обязательным признаком субъективной стороны любого преступления является вина. Принцип виновной ответственности закреплен в ст. 5 УК РФ. Вина представляет собой психическое отношение лица к совершаемому им общественно опасному деянию, предусмотренному уголовным законом, и его последствиям. В ней проявляется отрицательное отношение лица к интересам (ценностям), охраняемым уголовным законом от преступных посягательств. Данное отрицательное отношение может проявляться в антисоциальной, асоциальной либо недостаточно выраженной социальной установке этого лица относительно важнейших ценностей общества. Вина проявляется в различных формах, т.е. в разнообразном сочетании признаков воли и сознания, характеризующих поведение лица. Как отмечают специалисты, принцип субъективного вменения, составляющий основу уголовного права и практики его применения, требует выяснения всех особенностей побудительных мотивов, направивших лицо на совершение преступления.

Любое преступление есть совокупность объективных и субъективных факторов. Только человек может совершать преступные деяния в объективном мире, но при этом должно быть единство его сознания и воли. Если нет этого единства, то либо это психически нездоровый человек, либо в его действиях нет вины. Таким образом, внутренняя деятельность, проявляющаяся в психике человека во время совершения им преступления, которая так и называется психической, является, на наш взгляд, важнейшим признаком в совокупности таковых при совершении человеком различных поступков, в том числе и преступления. Эта осознанная деятельность субъекта относится к так называемой субъективной стороне состава преступления. Следует поддержать позицию А.И. Рарога, согласно которой под субъективной стороной преступления в науке уголовного права

понимается "психическая деятельность лица, непосредственно связанная с совершением преступления"[1].

При расследовании преступления необходимо в поведении человека, в его отношении к совершенному посягательству и наступившим последствиям установить наличие обязательных и факультативных признаков субъективной стороны преступления и только тогда сделать вывод о виновном совершении преступления. Хотя вывод может быть и прямо противоположным. Возможно, поэтому очень часто понятие субъективной стороны уравнивают с понятием вины. Нельзя путать элемент состава преступления как законодательной модели и признак, раскрывающий содержание данного элемента.

В литературе высказывалось мнение о том, что субъективная сторона преступления включает и такие признаки, как эмоции, аффект и заведомость. Однако это суждение правильно лишь в отношении эмоционального состояния. Таким образом, содержание субъективной стороны преступления исчерпывается в большей степени следующими признаками: виной, мотивом и целью.

Вина, являясь субъективным основанием уголовной ответственности, - основной юридический признак, характеризующий психическое содержание любого преступления, представляющий собой психическое отношение лица к совершенному общественно опасному деянию и к его общественно опасным последствиям. Содержание вины составляют интеллектуальный и волевой моменты, различные соотношения которых, закрепленные в законе, образуют разные формы вины.

Все хищения являются умышленными преступлениями, при совершении которых вина преступника выражается только в виде прямого умысла. Согласно ст. 25 УК РФ, преступление признается совершенным с прямым умыслом, если лицо осознавало общественную опасность своих

---

[1] Рарог А.И. Субъективная сторона и квалификация преступлений. М., 2001. С. 6.

действий (бездействия), предвидело возможность или неизбежность наступления общественно опасных последствий и желало их наступления.

Таким образом, в предметное содержание прямого умысла при совершении хищения в форме кражи, мошенничества, присвоения, растраты и грабежа входит совокупность трех признаков: осознание того, что тайным, открытым ненасильственным либо открытым насильственным способом, путем обмана или злоупотребления доверием, присваивая или растрачивая, противоправно и безвозмездно виновный изымает чужое имущество и обращает его в свою пользу или пользу других лиц; субъект преступления реально предвидит возможность или неизбежность причинения в результате своих противозаконных действий прямого имущественного ущерба собственнику или иному лицу; виновный желает обратить чужое имущество в свою пользу или в пользу других лиц, причинив при этом имущественный ущерб собственнику.

Следует отметить: законодательное определение прямого умысла ориентировано только на преступления с материальным составом, где желание виновного связывается только с общественно опасными последствиями, в которых воплощен вред, причиняемый объекту. Осознание виновным общественно опасного характера, совершаемого им деяния, является интеллектуальным элементом прямого умысла. Сознавать - значит не только знать о фактических обстоятельствах (признаках) совершаемого деяния, но и иметь представление о характере тех благ, на которые совершается посягательство, т.е. об объекте преступления. Определяя предметное содержание умысла, Ю.А. Демидов отмечает, что фактические обстоятельства, охватываемые умыслом, могут относиться к общественно опасному действию (бездействию) и к его общественно опасным последствиям[1]. Таким образом, время, место, обстановка, способ и другие обстоятельства, относящиеся к действию или бездействию, являясь

[1]Демидов Ю.А. Предметное содержание умысла по советскому уголовному праву // Труды ВШ МООП. М., 1965. N 12. С. 29.

качественными признаками деяния, становятся предметом сознания при умысле. Так, лицо, совершая карманную кражу, должно осознавать тайный способ завладения чужим имуществом, обстановку совершения указанного преступления (совершение кражи в присутствии потерпевшего). Предвидение общественно опасных последствий - мысленное представление виновного о том вреде, который причинит или может причинить его деяние общественным отношениям, поставленным под защиту уголовного закона. Желание наступления последствий как волевой элемент прямого умысла - это воля, мобилизованная на достижение цели, стремление к определенному результату[1].

Таким образом, мы приходим к выводу о том, что лица, совершающие мошенничество с использованием компьютерной информации, действуют с прямым, четко определенным, заранее обдуманным умыслом. Это в полной мере соответствует разъяснению Пленума Верховного Суда РФ, согласно которому содеянное следует квалифицировать как мошенничество, если умысел, направленный на хищение чужого имущества или приобретение права на чужое имущество, возник у лица до получения чужого имущества или права на него[2].

§3. Квалифицирующие признаки состава преступления

[1]Карпова Н.А. Хищение чужого имущества: проблемы дифференциации уголовной ответственности и вопросы квалификации: Научно-практическое пособие / Под ред. проф. Н.Г. Кадникова. М.: Юриспруденция, 2011. С. 90.

[2]Постановление Пленума Верховного Суда Российской Федерации N 51 от 27 декабря 2007 г. "О судебной практике по делам о мошенничестве, присвоении и растрате".

Действующее уголовное законодательство, определяя понятие мошеннического посягательства, предусматривает ряд обстоятельств, при наличии которых рассматриваемое преступление признается более опасным для общества. Эти обстоятельства учтены законодателем в качестве квалифицирующих признаков мошеннического посягательства.

К квалифицированному виду мошеннического посягательства, предусмотренного ч.2 ст.159.6 УК России, относится мошенничество, совершенное:

а) группой лиц по предварительному сговору;

б) с причинением значительного ущерба гражданину.

Часть 3 ст.159.6 УК России говорит о более опасных для общества квалифицированных видах мошенничества, совершенных:

а) лицом с использованием своего служебного положения;

б) в крупном размере

Часть 4 ст.159.6 УК России говорит о еще более опасных для общества квалифицированных видах мошенничества, совершенных:

а) организованной группой

б) в особо крупном размере;

Мошенничество признается совершенным группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении этого преступления. Обычно такой сговор происходит относительно места, времени или личности потерпевшего. Предварительным считается сговор, состоявшийся до начала мошенничества, во время приготовления к нему или непосредственно перед покушением. Промежуток времени между сговором и началом мошеннического посягательства не имеет значения. Присоединение лица к уже начатому мошенничеству с последующим сговором о совместном

окончании преступления не дает основания усматривать здесь данный квалифицирующий признак.

По признаку группы с предварительным сговором могут квалифицироваться действия также тех лиц, которые непосредственно участвовали в совершении мошеннического посягательства как соисполнители преступления. При этом необязательно, чтобы все они выполняли одинаковые действия. Действия соисполнителей квалифицируются без ссылки на ст. 33 УК России.

Действия лиц, которые непосредственно не участвовали в совершении мошенничества, а ограничились подстрекательством или обещанием скрыть похищенное, или иным путем содействовать мошеннику, должны квалифицироваться по ч.4 и ч.5 ст. 33 и ст.159.6 УК России.

Мошенничество признается совершенным с использованием виновным своего служебного положения в случае, если для изъятия и (или) обращения чужого имущества либо приобретения права на него субъектом была использована занимаемая им должность в любых учреждениях или организациях независимо от формы собственности. При этом не имеет значения, является ли виновный должностным лицом либо лицом, выполняющим управленческие функции в коммерческой или иной организации.

Мошенничество, совершенное с причинением значительного ущерба гражданину, может иметь место при посягательствах на частную собственность каждого лица в отдельности. Например, значительным ущербом для гражданина может признаваться ущерб равный сумме, которую гражданин не может покрыть за месячную заработную плату, а так же учитывается финансовое положение семьи потерпевшего, но не менее 5000 рублей. В этом состоит особенность данного квалифицирующего признака по сравнению с другими, установление которых не зависит от формы собственности.

Мошенничество признается совершенным организованной группой, если оно "совершено устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений" (ст. 35 УК России). Пленум Верховного Суда России в постановлении №5 от 25 апреля 1995 года "О некоторых вопросах применения судами законодательства об ответственности за преступления против собственности" отметил, что такая группа характеризуется, как правило, высоким уровнем организованности, планированием и тщательной подготовкой преступления, распределением ролей между соучастниками.

Отличительным признаком данной группы является устойчивость, которая обычно предполагает умысел соучастников на совершение не одного, а нескольких преступлений. Устойчивость также проявляется в наличии руководителей, в предварительной подготовке преступных деяний, в подборе соучастников и распределении ролей между ними, в обеспечении мер по сокрытию преступлений, в наличии отработанных методов преступной деятельности.

Согласно ч. «б» ст. 35 УК России, создание организованной группы в случаях, специально не предусмотренных Особенной частью УК России, влечет ответственность за приготовление к тем преступлениям, для совершения которых она создана. В соответствии с ч. «5» ст. 35 УК России лица, создавшие организованную группу или преступное сообщество, либо руководившие ими, подлежат ответственности за их организацию и руководство в случаях, предусмотренных Особенной частью УК России, а также за все совершенные организованной группой или преступным сообществом преступления, если они охватывались их умыслом. Другие участники организованной группы или преступного сообщества несут ответственность за участие в них в случаях, предусмотренных Особенной

частью УК России, а также за преступления, в подготовке или совершении которых они участвовали[1].

Мошенничество с использованием компьютерной информации (159.6 УК России) признается совершенным в крупном размере в случае, если стоимость похищенного имущества, превышает 1 500 000 рублей, а в особо крупном размере от 6 000 000 руб. и выше.

Совершение нескольких хищений чужого имущества путем обмана или злоупотребления доверием, образующих в общей сложности крупный размер, если содеянное свидетельствует о едином продолжаемом преступлении (все мошеннические действия совершены одним способом и при обстоятельствах, свидетельствующих об умысле совершить хищение в крупных размерах), надлежит квалифицировать как хищение в крупном размере.

Говоря о совершении мошенничества в крупных, размерах, следует отметить, что при совершении мошенничества группой лиц размер хищения определяется общей стоимостью похищенного имущества без учета фактически полученной доли каждым из соучастников. Если же отдельные соучастники принимали участие не во всех эпизодах хищения, то квалификация их действий должна зависеть от размера ущерба, причиненного теми преступлениями, в которых они участвовали.

Необходимо также рассмотреть момент покушения и окончания преступления, так как это влияет на квалификацию мошенничества с использованием компьютерной информации как неоконченного преступления.

Прежде всего следует отметить, что ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей в

[1] Ледяев А.П. Классификация криминалистически значимых признаков организованного мошенничества./ Российский судья. 2011, № 9. С. 28.

зависимости от конкретных обстоятельств дела может содержать признаки как приготовления к мошенничеству в сфере компьютерной информации, так и покушения на совершение этого преступления. При этом отграничение приготовительных действий от покушения не всегда представляется столь очевидным.

Как известно, признак создания условий для совершения преступления является ключевым при отграничении приготовления к преступлению от покушения на преступление. Например, создание вредоносной компьютерной программы или ее распространение через информационно-телекоммуникационную сеть в целях последующего совершения мошенничества следует оценивать, как приготовление к преступлению. По своему характеру приготовительными также являются действия по созданию сайтов-двойников и иных онлайн-ловушек, направленных на копирование персональной информации пользователей.

Вместе с тем совершение манипуляций с компьютерной информацией, непосредственно направленных на изъятие имущества, свидетельствует о выполнении лицом объективной стороны преступления, предусмотренного статьей 159.6 УК РФ. Если по независящим от виновного обстоятельствам (сбой оборудования, ошибка в работе программного обеспечения, блокировка трансакции системой безопасности банка, пресечение действий сотрудниками правоохранительных органов и др.) деяние не было доведено до конца, содеянное необходимо квалифицировать как покушение на мошенничество в сфере компьютерной информации. Так, по одному из дел о покушении на мошенничество в сфере компьютерной информации суд указал, что довести общий преступный умысел лица до конца не смогли по независящим от них обстоятельствам, так как сотрудниками банка трансакция не была проведена[1].

---

[1] См.: уголовное дело N 1-43/2014 // Архив Пресненского районного суда г. Москвы. См.: уголовное дело N 1-43/2014 // Архив Пресненского районного суда г. Москвы.

Как покушение на совершение компьютерного мошенничества следует оценивать и случаи, когда лицо не имело возможности распорядиться похищенным имуществом вследствие того, что, например, расчетный счет в банке, на котором аккумулировались денежные средства, изначально был заблокирован кредитной организацией.

На наш взгляд, позиция, сформулированная в Постановлении Пленума Верховного Суда РФ от 27 декабря 2007 г. N 51 "О судебной практике по делам о мошенничестве, присвоении и растрате", согласно которой с момента зачисления денег на банковский счет лица оно получает реальную возможность распоряжаться поступившими денежными средствами по своему усмотрению, может иметь вполне конкретные исключения. Иными словами, представляется возможной ситуация, когда деньги на счет виновного могут поступить, но реальная возможность по их распоряжению не возникнет (например, в случае блокировки счета по совершению расходных операций).

ГЛАВА II. ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, ПРЕДУСМОТРЕННЫХ СТАТЬЕЙ 159.6 УК РФ И ОТГРАНИЧЕНИЕ ЕГО ОТ СМЕЖНЫХ СОСТАВОВ

§1. Отграничение мошенничества с использованием компьютерной информации от смежных составов преступления

С развитием и повсеместным внедрением сети Интернет появились новые возможности ее использования. Однако все это с неизбежностью привело и к расширению сферы деятельности для правонарушителей и появлению новых видов преступных посягательств, в том числе такого, как мошенничество с использованием компьютерной информации.

Виды преступной деятельности, в которой компьютерная информация выступает в качестве орудия совершения преступления или предмета преступного посягательства, настолько разнообразны, что компьютерная преступность по новому уголовному законодательству Российской Федерации стала объектом исследования многих юридических наук, в частности, уголовного права, криминологии, криминалистики, оперативно-разыскной деятельности.

Неслучайно на заседании коллегии МВД России 22 мая 2014 г. были рассмотрены проблемы выявления, раскрытия и расследования преступлений, совершенных с использованием современных информационных технологий, а также разработаны организационно-управленческие и иные меры их решения.

Действительно, хищения денежных средств с пластиковых карт посредством различных компьютерных информаций представляют собой значимую общественную опасность.

В связи с чем 10 декабря 2012 г. в Уголовном кодексе РФ начали действовать новые статьи, выделяющие в отдельные виды преступлений мошенничества, связанные с использованием банковских услуг. Теперь как отдельные преступления классифицируются мошенничества в сфере кредитования, с использованием платежных карт, интернет технологий.

«Принятый Государственной Думой Федеральный закон позволит снизить ошибки и злоупотребления во время возбуждения уголовных дел о мошенничестве, будет способствовать повышению качества работы по выявлению и расследованию таких преступлений, правильной квалификации содеянного органами предварительного расследования и судом, более четкому отграничению уголовно наказуемых деяний от гражданско-правовых отношений» - *Заключение Комитета Совета Федерации по конституционному законодательству, правовым и судебным вопросам*[1].

С момента дополнения Уголовного кодекса РФ шестью новыми составами, предусматривающими ответственность за различные виды мошенничества, вопрос целесообразности этих новелл был актуальной темой дебатов на протяжении долгого времени и остается таковой по сей день.

Мошенничество в сфере компьютерной информации с каждым годом становится все более распространенным преступлением, при этом недостаточная осведомленность правоприменителей об особенностях подобного деяния приводит к ошибкам в квалификации. Отрицательно сказывается на следственной и судебной практике тот факт, что отсутствуют четкие разъяснения на уровне ВС РФ, решающие проблемы разграничения

---

[1] Мошенничество в платежной сфере: Бизнес-энциклопедия / Центр исследований платежных систем и расчетов. — М.: Интеллектуальная Литература, 2016. — С.136

смежных составов и другие спорные вопросы квалификации, касающиеся особенностей объективной стороны, а также предмета преступления.

Изучение уголовных дел показало, что хищения, совершаемые путем использования компьютерной информации, можно разделить на группы в зависимости от способа их совершения:

1) преступления с использованием услуги "Мобильный банк" посредством мобильной связи:

- телефон выбывает из владения собственника по различным причинам (утрата телефонного аппарата либо его хищение), при этом потерпевший не отключает услугу "Мобильный банк" от сим-карты и преступник получает возможность производить манипуляции с денежными средствами, пользуясь данной услугой;

- потерпевшим производится замена номера телефона, при этом сим-карта остается прежней, либо потерпевшим в течение нескольких месяцев сим-карта с подключенной услугой "Мобильный банк" не используется, после чего продается компанией сотовой связи новому владельцу, который, получая смс-сообщения с номера "900", имеет возможность осуществлять операции с денежными средствами на счетах потерпевшего;

- посредством программы-вируса;

- путем обмана через смс-сообщения о блокировке карты, имеющейся задолженности, либо об отсутствии денежных средств на карте, либо о заявке на перевод денежных средств с указанием контактного телефона;

2) преступления, связанные с приобретением товаров и услуг посредством сети Интернет либо возвратом утраченного имущества за вознаграждение, когда потерпевшие перечисляют денежные средства на телефонные номера либо на банковские счета преступников;

3) преступления, связанные с перечислением денежных средств на покупку товара, приобретение товаров и услуг посредством сети Интернет, когда потерпевшие сами перечисляют денежные средства на телефонные номера либо на банковские счета преступников.

Особенность указанных видов мошенничества в том, что при их совершении преступниками активно используется компьютерная информация. Именно компьютерная информация, зачастую не являясь предметом посягательства, представляет собой обязательный элемент способа его совершения. Под компьютерной информацией следует понимать сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Поэтому ошибочно мнение правоприменителей, утверждающих, что квалифицировать по ст. 159.6 УК РФ следует только деяния, совершаемые посредством сети Интернет. Так называемые телефонные мошенничества необходимо также относить к разряду преступлений, совершаемых в сфере компьютерной информации. Однако кроме компьютерной информации следует обратить внимание на другие особенности, для того чтобы определить, будет являться содеянное мошенничеством или иным видом хищения.

Способами компьютерного мошенничества являются ввод, модификация, блокирование, удаление компьютерной информации и вмешательство в функционирование средств хранения, обработки и передачи информации, а также информационно-телекоммуникационных сетей. Данные способы включают взлом паролей, кражу номеров кредитных карточек и других банковских реквизитов (фишинг). Кроме того, распространенным видом мошенничества являются Интернет-аукционы, в которых сами продавцы делают ставки, чтобы поднять цену выставленного на аукцион товара.

Схема компьютерного мошенничества заключается в том, что преступник умышленно с целью хищения имущества потерпевшего осуществляет доступ к защищенной информации, не имея на это правомочий.

Каспийским городским судом Республики Дагестан привлечен к уголовной ответственности по ч. 2 ст. 159.6 УК РФ И., который с

использованием персонального компьютера, подключенного к сети Интернет, с принадлежащего Р. электронного счета 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 обналичил посредством снятия через банкомат, причинив таким образом ущерб потерпевшему Р.[1]

Нижегородским городским судом Л. привлечена к уголовной ответственности по ч. 3 ст. 159.6 УК РФ. У Л., работавшей в филиале банка в должности старшего специалиста отдела по работе с корпоративными клиентами, в июне 2012 года возник преступный умысел, направленный на хищение денежных средств, принадлежащих клиентам банка. Для реализации преступного умысла Л. перевела денежные средства, находящиеся на лицевых счетах ключевых клиентов, на подконтрольные ей лицевые счета, оформленные по несуществующим анкетным данным, провела финансовую корректировку с использованием автоматизированной системы расчетов Marti и затем перечислила указанные денежные средства на имеющиеся у нее банковские карты при помощи сервиса "Легкий платеж". Далее Л. по несуществующим анкетным данным создала несколько лицевых счетов на имя Б. и Ж. Согласно условиям работы сервиса "Легкий платеж" для осуществления перевода денежных средств с абонентом, т.е. с физическим лицом, должен быть заключен абонентский договор, в соответствии с которым максимальная сумма одной операции по абонентскому номеру составляет не более 14999 рублей, максимальная общая сумма платежей в сутки - не более 30000 рублей. Таким образом, для осуществления своих преступных намерений с целью извлечения максимально возможной выгоды Л. неоднократно осуществляла операции по смене абонентского номера на лицевых счетах для получения возможности

[1] Приговор Каспийского городского суда Республики Дагестан по делу Р. URL: http://www.sudrf.ru

проводить большее количество операций. Всего Л. по лицевому счету 1 на имя Б. произведено 24 операции по замене абонентского номера, по лицевому счету 1 на имя Ж. - 31, по лицевому счету 2 на имя Б. - 14, по лицевому счету 2 на имя Ж. - 21 [1].

Таким образом, в период с июня по ноябрь 2012 года Л. с лицевых счетов ключевых клиентов похитила путем переноса на лицевые счета на имя Б. и Ж. денежные средства на общую сумму 2613581 рублей 73 копейки. Продолжая реализовывать свой преступный умысел, направленный на хищение денежных средств, Л. провела финансовые корректировки на счетах ключевых клиентов, мотивировав это тем, что был применен неправильный тариф, при этом достоверно зная, что тарификация была произведена корректно, и таким образом модифицировала компьютерную информацию. Похищенные денежные средства Л. перевела на имеющиеся у нее банковские карты и использовала их по собственному усмотрению.

Также нами рассмотрены разъяснения, данные в постановлении Пленума Верховного Суда РФ от 27.12.2007 N 51 "О судебной практике по делам о мошенничестве, присвоении и растрате". В них указывается, что в случаях, когда мошенничество сопряжено с неправомерным внедрением в чужую информационную систему или с иным неправомерным доступом к охраняемой законом компьютерной информации кредитных учреждений либо с созданием заведомо вредоносных программ для электронно-вычислительных машин, внесением изменений в существующие программы, использованием или распространением вредоносных программ для ЭВМ, содеянное подлежит квалификации по статье 159 УК РФ, а также, в зависимости от обстоятельств дела, по статьям 272 или 273 УК РФ, если в результате неправомерного доступа к компьютерной информации произошло

[1] Приговор Нижегородского городского суда по делу Л. URL: http://www.sudrf.ru

уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети[1].

Как показывает практика, чаще всего ст. 159.6 УК РФ применяется по совокупности со ст. 272 УК РФ, предусматривающей ответственность за неправомерное завладение компьютерной информацией. Так, для хищения "электронных денег" преступнику необходимо сначала получить код доступа. Однако подобная квалификация вызывает сомнение у ряда ученых. Например, Р.Д. Шарапов полагает, что "по существу неправомерный доступ к охраняемой законом компьютерной информации в целях хищения чужого имущества или приобретения права на чужое имущество является способом нового вида мошенничества в сфере компьютерной информации.

Обсуждая вопрос о квалификации содеянного по ст. 272 УК РФ, следует отметить, что в законе отсутствует системность при установлении наказания за преступное хищение, сопряженное с незаконным использованием компьютерной информации, но без признаков хищения: мошенничество, причинившее ущерб до 10000 рублей, карается мягче, чем преступление, предусмотренное ч. 1 ст. 272 и ч. 1 ст. 273 УК РФ. В то же время преступление, предусмотренное ч. 2 ст. 159.6 УК РФ, подлежит более жесткому наказанию, чем деяние, ответственность за которое предусмотрена ч. 1 ст. 272, и соразмерно наказанию за преступление, описанное в ч. 2 ст. 273 УК РФ.

Представляется, что решить вопрос о конкуренции ст. 159.6 и ч. 2 ст. 272 УК РФ можно исходя из последствий преступления: в случае, когда действия преступника направлены на завладение чужим имуществом, необходимо осуществлять квалификацию по ст. 159.6 УК РФ, когда же в процессе хищения имущества компьютерная информация уничтожается, блокируется, модифицируется либо копируется, требуется квалификация по

---

[1] Постановление Пленума Верховного Суда РФ от 27.12.2007 N 51 "О судебной практике по делам о мошенничестве, присвоении и растрате"//Бюллетень Верховного Суда РФ, N 2, февраль, 2008.

ч. 2 ст. 272 УК РФ. Аналогичная квалификация должна проводиться и при использовании для хищения имущества вредоносных компьютерных программ (ст. 273 УК РФ).

В ряде случаев правоприменитель квалифицирует сообщение ложных сведений по телефону как мошенничество, а действия, не сопровождающиеся обманом, как кражу. Попытаемся на конкретном примере разобрать, как следует квалифицировать и разграничивать указанные деяния.

В 2013 году Грачевским районным судом Ставропольского края вынесен приговор в отношении Н., которая своими умышленными действиями совершила мошенничество в сфере компьютерной информации при следующих обстоятельствах. Получив на мобильный телефон электронное сообщение посредством услуги "Мобильный банк" о доступном лимите денежных средств на не принадлежащем ей банковском счете, открытом на имя Ш., имея умысел на хищение данных средств и реализуя его, используя принадлежащий ей мобильный телефон "Samsung" и сим-карту с абонентским номером, зарегистрированным на имя Д., к которой ошибочно подключена услуга "Мобильный банк" Сбербанка России, предоставляющая право распоряжаться денежными средствами, находящимися на расчетном счете на имя Ш., путем ввода компьютерной информации в форме электрических сигналов - "смс-сообщения" (здесь и далее выделено нами. - Е.Б.) на номер "900" посредством телекоммуникационной сети оператора сотовой связи "О", перечислила (похитила) денежные средства, находившиеся на расчетном счете и принадлежащие Ш., на счет сим-карты. Продолжая свои преступные действия, направленные на хищение денежных средств, Н. путем ввода компьютерной информации в форме электрических сигналов - "смс-сообщения" на номер "7878" по услуге денежных переводов, предоставленной провайдером "mobi деньги RU/RU", с учетом вычета комиссии перевела денежные средства на счет сим-карты с абонентским

номером, зарегистрированным на ее имя, тем самым распорядилась ими по своему усмотрению, причинив Ш. имущественный ущерб[1].

В данном случае суд подчеркивает способ совершения преступления: путем ввода компьютерной информации в форме электрических сигналов - "смс-сообщения", тем самым указывая на то, что преступление совершено именно с использованием компьютерной информации. Необходимо акцентировать на этом внимание, поскольку на сегодняшний день распространена ошибка первоначальной квалификации подобных описанному выше деяний по ст. 159 УК РФ.

Кроме того, следует отграничивать мошенничество в сфере компьютерной информации от кражи. К примеру, изъятие из банкомата денег посредством похищенной пластиковой карты правоприменителем в настоящее время квалифицируется как кража. Однако доктрина уголовного права не позволяет квалифицировать как кражу хищение имущества, не отвечающего признакам вещи (в том числе права на имущество). Завладение пластиковой картой позволяет преступнику получить право на имущество, а затем, осуществляя неправомерный ввод компьютерной информации в систему ("взлом"), получить доступ к денежным средствам. Указанные деяния квалифицируются по ст. 158 УК РФ, поскольку Пленум Верховного Суда РФ в п. 13 Постановления от 27.12.2007 N 51 "О судебной практике по делам о мошенничестве, присвоении и растрате" (далее - Постановление Пленума ВС РФ N 51) указывает на обязательный признак мошенничества - наличие обманутого физического лица[2]. Однако в пояснительной записке к законопроекту от 11.04.2012 "О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации" (о выделении самостоятельных составов мошенничества) ВС РФ

---

[1] Приговор Грачевского районного суда Ставропольского края по делу Н. URL: http://www.sudrf.ru

[2] Постановление Пленума ВС РФ от 27.12.2007 N 51 "О судебной практике по делам о мошенничестве, присвоении и растрате" // Российская газета. 2008.

разъясняет, что подобное преступление совершается не путем обмана или злоупотребления доверием конкретного субъекта, а посредством получения доступа к компьютерной системе и совершения любого действия, прописанного в диспозиции ст. 159.6 УК РФ[1]. Исходя из предложенных разъяснений завладение денежными средствами потерпевшего посредством банковской карты следует квалифицировать как мошенничество в сфере компьютерной информации. Нужно отметить, что квалификация подобного деяния меняется на ст. 159.3 УК РФ "Мошенничество с использованием платежных карт", если оно совершено путем обмана уполномоченного работника кредитной, торговой или иной организации.

В ряде случаев завладение денежными средствами потерпевшего посредством услуги "Мобильный банк" также признается кражей. К примеру, Пермский районный суд квалифицировал по п. "в" ч. 2 ст. 158 УК РФ действия Ш., который, пользуясь абонентским номером с подключенной услугой "Мобильный банк", тайно из корыстных побуждений путем перевода денежных средств с банковской карты "Маэстро" Сбербанка России на счет другого абонентского номера похитил денежные средства на общую сумму 9611 рублей, принадлежащие потерпевшей М. Впоследствии Ш. распорядился похищенными денежными средствами по своему усмотрению[2].

Представляется, что в данном случае правоприменителем не проанализированы нормы закона, разъяснения, а также не учтена наработанная судебная практика по данному вопросу, что привело к ошибочной квалификации.

Одним из часто возникающих проблемных вопросов является отсутствие в диспозиции ст. 159.6 УК РФ указания на такие способы совершения преступления, как обман или злоупотребление доверием. В

---

[1] Пояснительная записка к проекту Федерального закона от 11.04.2012 N 53700-6 "О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации" // СПС "КонсультантПлюс".

[2] Приговор Пермского городского суда по делу Ш. URL: http://www.sudrf.ru

данном случае, поскольку ст. 159.6 УК РФ соотносится как специальная норма с общей, представляется, что указанный способ заложен в смысл ст. 159.6 УК РФ по умолчанию, исходя из определения термина "мошенничество", предлагаемого в диспозиции ст. 159 УК РФ.

Вызывает множество вопросов трактовка термина "иное вмешательство в функционирование средства хранения компьютерной информации", не имеющего конкретного определения и порождающего ошибки толкования и правоприменения. Полагаем, что под иным вмешательством следует понимать реализацию неправомерных действий, изменяющих установленный процесс обращения с компьютерной информацией, в том числе ее обработки, хранения, использования и передачи.

Кроме того, с технической точки зрения применение в законе термина "удаление информации" не совсем корректно. Так, затирание компьютерной информации не является удалением. Информация, по сути, просто скрыта. Данный факт не освобождает преступника от ответственности, поскольку затирание подпадает под иное вмешательство, однако отметим, что термин "уничтожение", используемый в ст. 272 УК РФ, более точно отражает особенности рассматриваемого деяния.

Раскрытие мошенничеств в сфере компьютерной информации осложняется тем, что ряд подобных деяний совершается лицами, отбывающими наказание в местах лишения свободы. Так, в 2015 году сотрудниками ОВД Иркутской области совместно с сотрудниками ГУФСИН по Иркутской области выявлена группа лиц, совершавшая мошенничество путем сообщения ложных сведений гражданам по телефону, в том числе в смс-сообщениях. Всего группой совершено около 30 преступлений в различных регионах России. Необходимо отметить, что в данном случае преступление следует квалифицировать как простое мошенничество по ст. 159 УК РФ, поскольку способом совершения данных преступлений являлось сообщение ложных сведений, но не работа с компьютерной информацией,

однако не следует исключать возможности совершения данными лицами хищений, связанных с использованием компьютерной информации.

Таким образом, мы видим, что мошенничество в сфере компьютерной информации с каждым годом становится все более распространенным преступлением. Однако, при этом недостаточная осведомленность правоприменителей об особенностях подобного деяния способствует некорректной квалификации данных видов преступлений. Мы считаем, что необходимо на уровне Верховного Суда РФ конкретное разграничение смежных составов, так как при возникновении сомнений правоприменителями возможна неправильная квалификация содеянного.

§2. Актуальные проблемы противодействия мошенничества в сфере компьютерной информации уголовно-правовыми средствами и пути их преодоления

Дискуссия о хищениях с использованием компьютерной информации идет давно, как высказывались и предложения о включении соответствующих статей в УК РФ[1]. Однако еще несколько лет назад такие предложения подвергались критике, а хищения с использованием компьютерной информации квалифицировались по совокупности с нормами главы 28 УК РФ. По мнению А.А. Комарова, глава 28 УК РФ выступает достаточно устойчивым конструктом, поскольку вменение статей по

[1] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Автореф. дис. ... к.ю.н. Владивосток, 2005. С. 13; Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: Дис. ... к.ю.н. Ижевск, 2002. С. 157 - 161.

совокупности в ряде случаев позволяет избежать внесения не вполне обоснованных изменений в УК, связанных с выделением отдельных видов компьютерной преступности в отдельных составах преступлений или повсеместного внедрения квалифицирующих признаков.

Включение указанной статьи в уголовное законодательство способствует конкретизации компьютерных преступлений, наряду с преступлениями в сфере компьютерной информации выделяя преступления, осуществляемые с использованием компьютерных средств. Однако включение данного состава преступления в уголовное законодательство Российской Федерации порождает также ряд проблем.

Так, в п. 12 Постановления Пленума Верховного Суда РФ от 27.12.2007 N 51 "О судебной практике по делам о мошенничестве, присвоении и растрате" говорится, что мошенничество с использованием компьютерной информации необходимо квалифицировать по совокупности ст. 159 УК РФ и ст. ст. 272 или 273 соответственно[1].

По прошествии времени приведенная выше позиция Верховного Суда РФ кардинально изменилась, в Постановлении Пленума от 05.04.2012 N 6 "О внесении в Государственную Думу Федерального Собрания Российской Федерации проекта Федерального закона "О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации" предложено ввести в УК РФ шесть новых статей, предусматривающих ответственность за различные виды мошенничества[2]. Одной из них явилась ст. 159.6 "Мошенничество в сфере компьютерной информации". Проект был поддержан законодателем, и Федеральным

---

[1] Постановление Пленума Верховного Суда РФ от 27.12.2007 N 51 "О судебной практике по делам о мошенничестве, присвоении и растрате" // СПС "КонсультантПлюс".

[2] Постановление Пленума Верховного Суда РФ от 05.04.2012 N 6 "О внесении в Государственную Думу Федерального Собрания Российской Федерации проекта Федерального закона "О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации" // URL: http:// www.vsrf.ru/

законом от 29.11.2012 N 207-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" в УК РФ были внесены соответствующие изменения. На наш взгляд, данная норма не только не решает существующие проблемы, но и может усугубить их.

1. Во-первых, само название ст. 159.6 не совсем корректно. Формулировка "сфера компьютерной информации" достаточно абстрактна, потому как нет четкого определения того, что под этой сферой понимается и что в нее входит. В связи с этим возникает вопрос, какие деяния можно отнести к мошенничеству в сфере компьютерной информации и что скрывается под определением предмета преступления как «информация».

Существует еще более широкое определение предмета преступления, когда он понимается уже не как нечто материальное, вещественное, а как любой из элементов общественного отношения. Сторонник такого взгляда на предмет Н.А. Беляев так обосновывает свою позицию: «Предмет посягательства — это элемент объекта посягательства, воздействуя на который преступник нарушает или пытается нарушить общественное отношение... Элементами общественного отношения являются... субъекты отношений, их деятельность, материальные вещи. Они и выступают в качестве предмета посягательства... Предметом посягательства может быть и сам преступник, если он является субъектом общественного отношения»[1].

Между тем, информация исключена из перечня объектов гражданских правоотношений с 01 января 2008 года[2]. В силу ряда свойств, у информации нет собственника, а только обладатель, что нашло свое отражение в ряде законов информационной отрасли права. Применяя понятие информационного объекта, информационной вещи, следует иметь в виду, что

---

[1] Беляев Н.А. Курс советского уголовного права. Общая часть. — Л., 1968.

[2] Статья 128 ГК РФ (в ред. Федерального закона от 18.12.2006 № 231-ФЗ).

информация, обладая стоимостью, не является имуществом как совокупности вещей.

Таким образом, вопрос о возможности рассмотрения информационной вещи в качестве предмета мошенничества, в настоящее не может решаться однозначно и нуждается в дальнейшей проработке. В рассматриваемой диспозиции, во всяком случае, как нами было сказано ранее, имеет место несогласованность в названии статьи 159.6 УК РФ и ее составом. Ничуть не проработан также вопрос об информации на носителе, могущей выступать в качестве «предмета», «вещи», «объекта».

В том, что касается возможности хищения денежных средств с использованием информационных систем, следует иметь в виду, что технологиями удаленного доступа к счетам предоставляется доступ к безналичным денежным средствам, а в момент, когда происходит обналичивание безналичных денежных средств, вопрос квалификации действий преступника следует разрешать в соответствии с Руководящими разъяснениями Пленума ВС РФ: «...Не образует состава мошенничества хищение чужих денежных средств путем использования заранее похищенной или поддельной кредитной (расчетной) карты, если выдача наличных денежных средств осуществляется посредством банкомата без участия уполномоченного работника кредитной организации. В этом случае содеянное следует квалифицировать по соответствующей части ст. 158 УК РФ»[1].

В научных статьях и исследованиях по рассматриваемой тематике, помимо понятия "компьютерное мошенничество", встречаются такие термины, как "кибермошенничество", "мошенничество в сети Интернет". Представляется, что термины "кибермошенничество" и "компьютерное мошенничество" являются синонимами. Так как в настоящий момент

[1] п.п. 12-14 Постановления Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ, № 2, февраль, 2008

понятия "компьютерное мошенничество" действующее законодательство не раскрывает, то данный термин носит лишь криминологический характер и понимается как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, совершенное с использованием средств компьютерной техники[1]. Что же касается мошенничества в сети Интернет, то это совокупность преступлений, характеризующихся единством способа совершения преступления (использование технологических и коммуникационных возможностей компьютерных систем, подключенных к глобальной сети Интернет, для совершения обмана человека или "обмана" компьютерной системы), а также корыстной мотивацией преступной деятельности. Таким образом, мошенничество в сети Интернет - разновидность компьютерного мошенничества.

Отдельно следует отметить мошенничество с использованием средств мобильной связи (телефонное или мобильное мошенничество), получившее достаточно широкое распространение в нашей стране. Мобильные телефоны также способны обрабатывать и хранить компьютерную информацию, с их помощью можно выйти в глобальную сеть Интернет. Кроме того, существуют и иные устройства, которые выполняют схожие с компьютером функции и также могут являться носителями компьютерной информации. Поэтому необходимо вести речь не о компьютерной, а об электронной информации, которая включает в себя информацию, обрабатываемую и в компьютерах, и в мобильных телефонах, и в иных схожих по функциям устройствах.

Пределы действия комментируемой нормы устанавливаются в том числе посредством толкования специальных терминов, с помощью которых описана объективная сторона деяния: компьютерная информация, средства ее хранения, обработки или передачи, информационно-

[1] Зыков Д. Понятие компьютерного мошенничества // Центр исследования проблем компьютерной преступности. URL: http://www.crime-research.org/library/Concept.htm

телекоммуникационные сети и их функционирование, ввод, удаление, блокирование, модификация компьютерной информации, иное вмешательство в функционирование указанных средств или сетей. К сожалению, указанные дефиниции в законодательстве в большинстве своем не раскрываются либо содержание их неточно.

Скажем, понятие компьютерной информации содержится в примечании 1 к ст. 272 УК, где под ней понимаются "сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи". Из такого определения следует, что данного вида информация - это такие сведения (сообщения, данные), которые хранятся, обрабатываются (систематизируются, становятся пригодными к выборке, передаче и др.) и передаются (стоило бы добавить, что и принимаются) с применением неких средств, которые также называют, в том числе в нормативных актах, машинными носителями[1], техническими устройствами и т.д.

Однако использование термина "электрический сигнал" в практике по уголовным делам затруднительно, во-первых, ввиду отсутствия у него нормативного содержания, а во-вторых, ввиду того что "возникают технологии, где устройства перестают быть электронными, а само понятие "электрический сигнал" теряет смысл. Уже используются биотехнологии, лазерные технологии, нанотехнологии и др."[2]; "информация, передаваемая по беспроводным и оптическим каналам связи, не подпадает под определение

---

[1] Статья 1 Федерального закона от 1 апреля 1996 г. N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования", п. 5 ч. 2 ст. 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

[2] Быков В., Черкасов В. Понятие компьютерной информации как объекта преступлений // Законность. 2013. N 12.

электрических сигналов при трактовке этого термина с точки зрения физики"[1].

Во-вторых, как нами ранее было заявлено, в целом компьютерные преступления условно можно разделить на две группы. Так, в первую группу входят преступления, в которых компьютерная информация является объектом преступления. Во вторую же группу входят те преступления, где информация является средством совершения преступления. Компьютерное мошенничество входит во вторую группу преступлений. Поэтому представляется, что целесообразной была бы такая формулировка, как "мошенничество с использованием электронной информации".

2. В соответствии с диспозицией ч. 1 ст. 159.6 УК РФ, мошенничеством в сфере компьютерной информации следует считать 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. На наш взгляд, здесь необходимы некоторые уточнения.

Правоприменительная практика уже неоднократно сталкивалась с проблемой, что же следует считать средствами хранения, обработки или передачи компьютерной информации, иногда к этим средствам относят даже кассовые аппараты.

Согласно п. 4 ст. 2 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

---

[1] Ефремова М.А. К вопросу о понятии компьютерной информации // Российская юстиция. 2012. N 7.

Ввиду отсутствия соответствующих законодательных дефиниций, а также разъяснений высшего судебного органа при применении ст. 159.6 УК целесообразно руководствоваться грамматическим значением используемых в тексте нормы слов, обозначающих способы хищения: ввод, удаление, блокирование, модификация компьютерной информации. Также при этом могут быть приняты во внимание предлагаемые Генеральной прокуратурой РФ рекомендации, согласно которым уничтожение информации - это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое "вытеснение" старых версий файлов последними по времени; блокирование информации - результат воздействия на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, т.е. совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением; модификация информации - внесение изменений в компьютерную информацию (или ее параметры)[1].

Модификацию компьютерной информации в силу частично бланкетного характера этого термина следует понимать и как изменение в программном обеспечении[2], посредством которого информация собирается, хранится, обрабатывается, передается, и как изменение в собственно информационном массиве. В последнем случае, однако, речь идет о такой

---

[1] См.: Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, утв. Генпрокуратурой России // http://genproc.gov.ru.

[2] Подпункт 9 п. 2 ст. 1270 ГК РФ.

модификации, в результате которой виновному удалось завладеть имуществом либо правом на имущество. В частности, как модификацию (изменение) компьютерной информации можно расценить такой результат действий виновного, который состоит в отражении в системе компьютерного учета сведений о распоряжении безналичными денежными средствами, как будто бы отданном уполномоченным на это лицом, например, гражданином - владельцем счета.

Перечень соответствующих признаков обсуждаемого преступления шире, нежели тот, что приведен в ст. 272 УК при описании общественно опасных последствий, наступивших в результате неправомерного доступа к охраняемой законом компьютерной информации (за исключением копирования, которое не является признаком компьютерного мошенничества). Этот перечень признаков мошенничества включает, во-первых, такой частный (но сопряженный со всеми остальными названными в норме действиями) случай проникновения в информационную среду, как ввод компьютерной информации, во-вторых, любые иные, помимо ввода, удаления, блокирования, модификации, виды вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации и, в-третьих, любое вмешательство в функционирование информационно-телекоммуникационных сетей.

Неясна такая формулировка, как "иное вмешательство" в функционирование вышеназванных средств.

Приведенную в законе формулу "вмешательство в функционирование" следует рассматривать как признак, содержащий критерий, существенно ограничивающий пределы действия комментируемой нормы. Так, если лицо путем доступа к содержащейся в компьютере информации (воспользовалось доступом к компьютеру, втайне от его пользователя раскрыло файл и ознакомилось с его содержанием) получило сведения, допустим, о паролях и логинах, позволяющих управлять счетом его владельца посредством системы "Банк-Клиент" (Онлайн-Банк и т.п.), но после ознакомления с указанной

информацией было задержано и в силу этого свой умысел на хищение до конца довести не смогло, то, поскольку в данном случае вмешательства именно в функционирование средств хранения, обработки или передачи компьютерной информации либо в функционирование информационно-телекоммуникационных сетей не произошло, содеянное признаков объективной стороны компьютерного мошенничества не образует и потому не может квалифицироваться как покушение на совершение указанного преступления. Даже если относить уже собственно доступ к компьютерной информации к объективной стороне мошенничества[1]. Содеянное в приведенном случае образует приготовление к компьютерному мошенничеству, что в силу ч. 2 ст. 30 УК будет влечь уголовную ответственность только при вменении лицу квалифицирующих признаков, предусмотренных ч. 4 ст. 159.6 УК РФ.

Признаком объективной стороны данного преступления является всякое вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, если его следствием стало незаконное завладение имуществом либо приобретение права на имущество. Когда, например, лицо, получив информацию о счетах граждан, изготавливало поддельные доверенности, получало дубликаты сим-карт и пароли, а затем, используя эти сим-карты и пароли, через электронную систему "*-Онлайн" путем перечисления на подконтрольные счета завладевало денежными

[1] Такая точка зрения встречается на практике, в ее обоснование приводится аналогия указанных действий с проникновением в помещение, хранилище или жилище, которыми начинается выполнение объективной стороны хищения. См.: п. 10 Постановления Пленума Верховного Суда РФ от 27 декабря 2002 г. N 29 "О судебной практике по делам о краже, грабеже и разбое".

средствами, как вмешательство было расценено собственно воздействие на информационную среду, которое ущерба ей не причинило[1].

3. Повсеместное внедрение информационно-телекоммуникационных технологий и информационных систем создало новые, уникальные возможности для активного и эффективного развития экономики и политики, государства, общества, граждан. Развитие информационных технологий в России, как и во всем мире, обусловило расширение сфер применения мобильных технологий, мобильных платежей, интернет-банкинга с подтверждением транзакций по SMS, SMS-банкингу и банковским мобильным приложениям в предпринимательской деятельности и в повседневной жизни. При этом быстрое развитие таких технологий создает предпосылки для их использования в преступных целях.

Неслучайно на заседании коллегии МВД России 22 мая 2014 г. были рассмотрены проблемы выявления, раскрытия и расследования преступлений, совершенных с использованием современных информационных технологий, а также разработаны организационно-управленческие и иные меры их решения.

Действительно, хищения денежных средств посредством различных компьютерных информаций представляют собой значимую общественную опасность.

Нами ранее, а именно в первой главе, были рассмотрены квалифицированные составы статьи 159.6 УК РФ. Так, ч. 2 ст. 159.6 устанавливает ответственность за те же деяния, совершенные группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину. По ч. 3 ст. 159.6 уголовной ответственности подлежит лицо, совершившее мошенничество в сфере компьютерной информации с использованием своего служебного положения, а равно в крупном размере.

---

[1] Апелляционное определение Московского городского суда от 6 мая 2013 г. N 10-2076. Однако, исходя из приведенного выше широкого понятия модификации компьютерной информации, можно заключить, что в данном случае такая модификация имела место.

Часть 4 ст. 159.6 предусматривает ответственность за те же деяния, совершенные организованной группой либо в особо крупном размере.

Следует отметить, что применительно к ст. 159 УК РФ крупным размером следует считать стоимость имущества, превышающую двести пятьдесят тысяч рублей, а особо крупным - один миллион рублей. Применительно же к ст. 159.6 УК РФ крупным размером признается стоимость имущества, превышающая один миллион пятьсот тысяч рублей, а особо крупным - шесть миллионов рублей, что в обоих случаях в шесть раз больше, чем в ст. 159 УК РФ.

При изучении нами выделенных в новый состав статей Уголовного Кодекса РФ (159.6, в том числе и 159.3 УК РФ) и при сравнении их со статьями кражи и мошенничества (158 и 159 УК РФ), можно выделить следующие аспекты:

1. Наказания за преступления, совершенные по новым статьям, значительно смягчены по сравнению с теми статьями, откуда они были выведены.

Статья УК РФ	Наказание			
	Часть 1	Часть 2	Часть 3	Часть 4
158 159	До 2 лет лишения свободы	До 5 лет лишения свободы	До 6 лет лишения свободы	До 10 лет лишения свободы
159.3 159.6	Арест до 4 месяцев	До 4 лет лишения свободы	До 5 лет лишения свободы	До 10 лет лишения свободы

2. Кроме смягчения наказания также были изменены и квалифицирующие величины ущерба. При их сравнении можно заметить тот факт, что законодателем усматривается, что причиненный ущерб от мошенничества в сфере компьютерной информации в 6 раз выше, чем от обычного мошенничества или кражи.

Статья УК РФ	Часть 3: в крупном размере	Часть 4: в особо крупном размере
158 159	250 000 руб.	1 млн руб.
159.3 159.6	1,5 млн руб.	6 млн руб.

Рассматривая санкции ст. 159.6 УК РФ, необходимо отметить, что они практически идентичны санкциям ст. 159 лишь за небольшим отличием: ч. 1 ст. 159.6 не предусматривает наказания в виде лишения свободы, в то время как ст. 159 предусмотрен такой вид наказания на срок до двух лет. В санкциях ч. ч. 2 и 3 ст. 159.6 наказание в виде лишения свободы присутствует и может быть назначено на срок до четырех и до пяти лет, против пяти и шести лет лишения свободы, предусмотренного в санкциях ч. ч. 2 и 3 ст. 159. Исходя из анализа санкций данных статей, видно, что мошенничество в сфере компьютерной информации является менее общественно опасным ввиду установления менее строгих санкций за его совершение. В то же время необходимо подчеркнуть, что мошенничество и мошенничество в сфере компьютерной информации различаются лишь по способу хищения чужого имущества или приобретения права на чужое имущество. Более того, если деяния, ответственность за которые предусмотрена ст. 159.6 УК РФ, совершены индивидуальным предпринимателем в связи с осуществлением им предпринимательской деятельности, либо членом органа управления коммерческой организации в связи с осуществлением им полномочий по управлению организацией, либо в связи с осуществлением организацией экономической деятельности, то уголовное дело может быть возбуждено не иначе как по заявлению потерпевшего или его законного представителя. Таким образом, в случае отсутствия заявления потерпевшей стороны лицо и вовсе сможет избежать уголовной ответственности, даже если совершит хищение в особо крупном размере, который, как отмечалось выше,

составляет сумму свыше 6 млн. руб. Очевидно, что сложившееся положение вещей не выдерживает критики.

Таким образом, мы видим, что за преступления, связанные с хищением денежных средств и иной материальных ценностей с помощью компьютерной информации и повлекшие за собой причинение значительного материального ущерба, которые представляют собой большую общественную опасность, преступнику могут быть применены наказания значительно меньше, чем за преступления, совершенные обычным мошенничеством или кражей.

Заключение

Компьютерное мошенничество получило свою популярность в 1970-е годы. Преступники начали активно использовать возможности новых технологий для взлома баз данных, в том числе банков и правительств. В связи с этим ряд государств дополняют свое уголовное законодательство нормами об ответственности за мошенничество, совершенное с помощью компьютерной информации и информационных технологий.

С момента дополнения Уголовного кодекса РФ шестью новыми составами, предусматривающими ответственность за различные виды мошенничества, число преступных посягательств на имущество, совершаемых путем обмана или злоупотребления доверием, продолжает расти.

С 2015 года в России зарегистрировано 196700 преступлений, ответственность за которые предусмотрена статьями 159 - 159.6 УК РФ (на 25% больше аналогичного периода 2014 года - 160214). На фоне общего роста числа зарегистрированных мошенничеств наблюдается значительный рост так называемых компьютерных мошенничеств, который составил 447% (с 995 по итогам 2014 года до 5443 в 2015 году). При этом раскрываемость последних по итогам 2015 года находилась на низком уровне и составляла лишь 7,4%. Также, рассматривая статистику мошенничества в сфере компьютерной информации, можно отметить, что к 2016 году на 3% преступность выросла в сравнении с 2015 годом, ущерб которого составил 235 млн рублей, что негативно складывается на социально-экономическом положении общества. В общей структуре правонарушений мошенничество занимает второе место.

1.Формулировка статьи 159.6 УК РФ, а именно «мошенничество в сфере компьютерной информации» представляется нам требующей изменения на «мошенничество с использованием электронной информации»

в связи с тем, что «сфера компьютерной информации» в составе преступления представляется узким положением.

В примечании 1 к ст. 272 УК РФ определяется, что под компьютерной информацией понимаются "сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи". Из такого определения следует, что данного вида информация - это такие сведения (сообщения, данные), которые хранятся, обрабатываются и передаются с применением неких средств, которые также называют, в том числе в нормативных актах, машинными носителями[1], техническими устройствами и т.д.

Однако использование термина "электрический сигнал" в практике по уголовным делам затруднительно, во-первых, ввиду отсутствия у него нормативного содержания, а во-вторых, ввиду того что "возникают технологии, где устройства перестают быть электронными, а само понятие "электрический сигнал" теряет смысл. Во-вторых, как нами ранее было заявлено, в целом компьютерные преступления условно можно разделить на две группы. Так, в первую группу входят преступления, в которых компьютерная информация является объектом преступления. Компьютерное мошенничество входит во вторую группу преступлений, где информация является средством совершения преступления.

В связи с этим, предлагаем диспозицию статьи 159.6 УК России изменить на следующую формулировку: «*мошенничество с использованием электронной информации*».

2.В ходе анализа уголовно-правовых норм об ответственности за преступления, совершаемые посредством компьютерной информации наглядно проглядывается проблематика в данной области.

---

[1] Статья 1 Федерального закона от 1 апреля 1996 г. N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования", п. 5 ч. 2 ст. 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

При изучении нами статьи УК РФ мошенничества в сфере компьютерной информации (159.6 УК РФ) и при сравнении его со статьями кражи и мошенничества (158 и 159 УК РФ) были выделены следующие проблематические аспекты:

- применительно к ст. ст. 158, 159 УК РФ крупным размером следует считать стоимость имущества, превышающую двести пятьдесят тысяч рублей, а особо крупным - один миллион рублей. Однако, в ст. 159.6 УК РФ крупным размером признается стоимость имущества, превышающая один миллион пятьсот тысяч рублей, а особо крупным - шесть миллионов рублей.

- наказания за преступления, совершаемые по статье 159.6 УК РФ, значительно смягчены по сравнению с той статьей, откуда он был выведен.

Рассматривая санкции ст. 159.6 УК РФ, необходимо отметить, что они практически идентичны санкциям ст. 159 УК РФ лишь за небольшим отличием: ч. 1 ст. 159.6 УК РФ не предусматривает наказания в виде лишения свободы, в то время как ст. 159 УК РФ предусмотрен такой вид наказания на срок до двух лет. В санкциях ч. ч. 2 и 3 ст. 159.6 УК РФ наказание в виде лишения свободы присутствует и может быть назначено на срок до четырех и до пяти лет, против пяти и шести лет лишения свободы, предусмотренного в санкциях ч. ч. 2 и 3 ст. 159 УК РФ.

Рассмотрев вышеизложенное, мы приходим к выводу, что законодатель применяет менее строгое наказание лицу, которое совершило преступление с более общественно опасным деянием.

В связи с этим, мы считаем необходимым внести следующие изменения в действующее уголовное законодательство:

Санкцию к ч. 2 ст. 159.6 УК РФ предусмотреть в виде лишения свободы на срок до 5 лет (действующая санкция: лишение свободы до 4 лет).

Санкцию к ч. 3 ст. 159.6 УК РФ предусмотреть в виде лишения свободы на срок до 6 лет (действующая санкция: лишение свободы до 5 лет).

Таким образом мы видим, что, не смотря на всю положительность распространения и внедрения в нашу жизнь компьютерных технологий и

информации мы приходим к пониманию опасности использования этих технологий в преступных целях. Существующее законодательство (в том числе уголовное) по охране нового вида общественных отношений (отношений в сфере компьютерной информации) от преступных посягательств еще недостаточно совершенно. Поэтому наша выпускная квалификационная работа являет собой попытку улучшения уголовного законодательства и выработке наиболее оптимальной схемы его применения в области борьбы с компьютерной преступностью.

Список использованной литературы:

Законы, нормативные правовые акты и иные официальные документы:

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с изм. и доп. от 21.07. 2014, №11-ФКЗ) // Российская газета. – 1993. – 25 дек.; Собрание законодательства РФ. – 2014. - №30 (ч.I), ст.4202.

2. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (с изм. и доп. от 17.04.2017 N 71-ФЗ) // Собрание законодательства РФ. – 1996. - №25, ст. 2954.

3. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 года N 51-ФЗ (с изм. и доп. от 28.03.2017 N 39-ФЗ): принят Гос. Думой 21 октября 1994 г. // Собрание законодательства РФ. 1994. - №32 ст. 3301.

4. Уголовный кодекс Австрии: принят 29 января 1974 г. Вступил в силу с 1 января 1975 г.: с изменениями и дополнениями на 1 мая 2013 г. СПб.: Юридический центр "Пресс", 2014. -350 с.

5. Уголовный кодекс Федеративной Республики Германия от 15.05.1871 (в ред. от 13 ноября 1998 г.). Особенная часть. СПб.: Юридический центр "Пресс", 2013. -524 с.

6. Уголовный кодекс Швеции от 01.01.1962 (в ред. от 2011 г.). / Под ред. С.С. Беляева, Н.Ф. Кузнецовой. СПб.: Юридический центр "Пресс", 2011. – 320 с.

7. Федеральный закон от 1 апреля 1996 г. N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования" // Собрание законодательства РФ от 1 апреля 1996 г. N 14 ст. 1401.

8. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" // Собрание законодательства Российской Федерации от 31 июля 2006 г. N 31 (часть I) ст. 3451.

9. Постановление Пленума Верховного Суда РФ от 27 декабря 2007 г. N 51 "О судебной практике по делам о мошенничестве, присвоении и растрате" // Российская газета от 12 января 2008 г. №4561.

10. Постановление Пленума Верховного Суда РФ от 05.04.2012 N 6 "О внесении в Государственную Думу Федерального Собрания Российской Федерации проекта Федерального закона "О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации" // URL: http:// www.vsrf.ru/

Монографии, учебники, учебные пособия:

11. Бакланов В.В, Пономарев М.Э. Опасная компьютерная информация / Учебно-методическое пособие. – Екатеринбург: в/ч 69617, 2013. – 180 с.

12. Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: Дис. ... к.ю.н. Ижевск, 2002. -189 с.

13. Беляев Н.А. Курс советского уголовного права. Общая часть. — Л., 1968 - 648 с.

14. Гаврилин Ю.В. Преступление в сфере компьютерной информации: квалификация и доказывание / Учебное пособие. М.: ЮИ МВД РФ, 2003. – 245 с.

15. Зубова М.А. Компьютерная информация как объект уголовно-правовой охраны: автореф. дис. … канд. юрид. наук: 12.00.08 / Зубова Марина Александровна. – Казань, 2008. – 29 с.

16. Карпова Н.А. Хищение чужого имущества: проблемы дифференциации уголовной ответственности и вопросы квалификации: Научно-практическое пособие / Под ред. проф. Н.Г. Кадникова. М.: Юриспруденция, 2014. - 184 с.

17. Косынкин А.А. Преодоление противодействия расследованию преступлений в сфере компьютерной информации: автореф. дис. … канд. юрид. наук: 12.00.09 / Косынкин Александр Александрович. – Саратов, 2012. – 24 с.

18. Курс уголовного права: В 5 т. Общая часть / Под ред. Н.Ф. Кузнецовой, И.М. Тяжковой. Особенная часть / Под ред. Г.Н. Борзенкова и В.С. Комиссарова. М.: Зерцало-М, 2002. - 2732 с.

19. Кудрявцев В.Н. Объективная сторона преступления. М., 1960. – 244 с.

20. Курс российского уголовного права. Особенная часть / Под ред. В.Н. Кудрявцева, А.В. Наумова. М.: Спарк, 2012. - 1040 с.

21. Медведев С.С. Мошенничество в сфере высоких технологий: дис... канд. юрид. наук / С.С. Медведев. - Краснодар, 2008. - 210 с.

22. Мошенничество в платежной сфере: Бизнес-энциклопедия / Центр исследований платежных систем и расчетов. / Под ред. А.С.Воронин. М.: Интеллектуальная Литература, 2016. — 430 с.

23. Ожегов С.И. Словарь русского языка. М., 2016. - 1200 с.

24. Орлов В.С. Субъект преступления по советскому уголовному праву. М., 1958. - 260 с.

25. Осокин Р.Б. Уголовно-правовая характеристика способов совершения мошенничества: Дис. ... канд. юрид. наук. М., 2004. - 184 с.

26. Преступность, уголовная политика, уголовный закон: сб. науч. тр./ под ред. Н.А. Лопашенко; Саратовский Центр по исследованию проблем организованной преступности и коррупции. Саратов: Изд-во ФГБОУ ВПО «Саратовская государственная юридическая академия», 2013 - 652 с.

27. Сало И.А. Преступные действия с компьютерной информацией ограниченного доступа: автореф. дисс. … канд. юрид. Наук: 12.00.08 / Сало Ирина Александровна. – М., 2012. – 24 с.

28. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Автореф. дис. ... к.ю.н. Владивосток, 2005. - 235 с.

29. Уголовное право России. Общая часть. Особенная часть: Учебник по специальностям "Правоохранительная деятельность", "Правовое обеспечение национальной безопасности"/ Под общ. ред. д.ю.н., проф. Н.Г. Кадникова. М.: ИД "Юриспруденция", 2013. - 929 с.

Статьи, научные публикации:

30. Быков В., Черкасов В. Понятие компьютерной информации как объекта преступлений // Законность. 2013. N 12. - С. 40

31. Елин В.М. Мошенничество в сфере компьютерной информации как новый состав преступления //Правовые вопросы бизнес-информатики. 2013. № 2. - С. 70-76

32. Ефремова М.А. К вопросу о понятии компьютерной информации // Российская юстиция. 2012. N 7. - С. 50-52

33. Иванченко Г.В., Малышев А.Н. Проблемы квалификации мошенничества в сфере компьютерной информации // Вестник Воронежского института МВД России 2014, №12

34. Кузнецов А. В. Совершенствование правового регулирования уголовной ответственности за отдельные виды мошенничества // Научный вестник Омской академии МВД России.2014 № 3. - С. 28-30

35. Ледяев А.П. Классификация криминалистически значимых признаков организованного мошенничества. / Российский судья. 2011, № 9. С. 28.

36. Степанов-Егиянц В.Г. Совершение кражи и мошенничества с использованием с компьютера или информационно-телекоммуникационных сетей // Финансовая жизнь, 2013, № 2. – С. 396

37. Филаненко А.Ю. Отграничения мошенничества в компьютерной информации от неправомерного доступа // Право и государство: теория и практика. 2013, №1. – С. 59-62

38. Хилюта В.В. Необходимость установления уголовной ответственности за хищения, совершаемые с использованием компьютерной техники/ В. В. Хилюта // Криминологический журнал, 2012, N 1. - С. 26-30.

39. Челноков В.В. Криминалистические аспекты последних изменений составов преступлений в сфере компьютерной информации // Актуальные проблемы теории и практики компьютерной криминалистики: материалы ведомственной научно-практической конференции – Екатеринбург: Институт ФСБ России. 2012. – С. 210-212

40. Шеслер А.В Мошенничество: проблемы реализации законодательных новелл // Уголовное право.2013. № 2. - С. 67-71

Материалы судебной, следственной практики:

41. Апелляционное определение Московского городского суда от 6 мая 2013 г. N 10-2076.

42. Архив Пресненского районного суда г. Москвы. // Уголовное дело N 1-43/2014

43. Приговор Грачевского районного суда Ставропольского края по делу Н. URL: http://www.sudrf.ru

44. Приговор Каспийского городского суда Республики Дагестан по делу Р. URL: http://www.sudrf.ru

45. Приговор Нижегородского городского суда по делу Л. URL: http://www.sudrf.ru

46. Приговор Пермского городского суда по делу Ш. URL: http://www.sudrf.ru

47. Приговор Хорошевского районного суда г. Москвы от 28 ноября 2014 г. по уголовному делу N 1-585/14 // http://судебныерешения.рф/bsr/case/6993929.

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

Отзыв
на выпускную квалификационную работу по теме «Актуальные вопросы квалификации кражи и мошенничества, совершаемые с использованием компьютерной информации», слушателя учебной группы №123 факультета подготовки специалистов по программам высшего образования Казанского юридического института МВД России младшего лейтенанта полиции Якупова Р.Р.

Выпускная квалификационная работа по теме «Актуальные вопросы квалификации кражи и мошенничества, совершаемые с использованием компьютерной информации», подготовленная слушателем факультета очного обучения Казанского юридического института МВД России младшего лейтенанта полиции Якупова Равиля Рамилевича, представляется весьма актуальной для сотрудников органов внутренних дел Российской Федерации, поскольку посвящена выработке практических знаний и умений по применению мер предупреждения и противодействия преступлений связанные с хищением, совершаемых с использованием компьютерной информации.

Автором верно отмечается, что преступления, совершаемые с использованием компьютерной информации, обладают повышенной общественной опасностью – представляют непосредственную и реальную угрозу не конкретному индивиду или организации, но и человечеству в целом, а их возрастание показывает несовершенство системы предупреждения этих преступлений, в том числе, уголовно-правовыми средствами. Не секрет, что преступления в сфере хищения имущества посредством компьютерной информации давно вышли за пределы отдельного государства и все больше приобретают транснациональный характер. Следовательно, противодействие данному виду преступлений стало одной из серьезных проблем, как для отечественных, так и для зарубежных правоохранительных органов.

Несомненной заслугой автора является комплексный подход к изучаемой проблеме. Автор демонстрирует хорошие теоретические знания и осведомленность в законодательной и правоприменительной практике по данному вопросу.

Убедителен автор в определении круга предметов преступлений, предусмотренных ст.ст. 158, 159.6 УК РФ.

Автор в своей работе прибегает к монографической и учебной литературу по рассматриваемой тематике, современное уголовное законодательство России, также различных периодов его развития, международные акты, законодательства зарубежных стран, опирается на материалы Постановлений Верховного Суда РФ, судебно-следственной практики, статистические данные.

Все вышесказанное свидетельствуют о несомненной актуальности выбора темы выпускной квалификационной работы.

Содержание выпускной квалификационной работы составляют введение, две главы (Уголовно-правовая характеристика мошенничества в сфере компьютерной информации; Вопросы квалификации преступлений, предусмотренных статьей 159.6 УК РФ и отграничение его от смежных составов), заключение, список использованных нормативных правовых актов, учебной и учебно-методической литературы.

Во введении выпускной квалификационной работы автором рассматривается уголовное законодательство зарубежных стран по предупреждению и противодействию хищениям, совершаемых посредством компьютерной информации, даётся общая характеристика оперативной обстановки в Российской Федерации, определяются актуальность, объект и предмет исследовательской работы. Таким образом, в начале дипломной работы Якуповым Р.Р. ставится проблема, изучение которой находит своё отражение в основной части выпускного квалификационного исследования. Здесь же указаны цели исследования и поставлены задачи, решение которых необходимо для их достижения.

В первой главе автором рассматривается анализ уголовно-правовой характеристики мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ). Изучаются особенности систематизации, а также квалификации норм об ответственности за преступления мошенничества в сфере компьютерной информации.

Вторая глава посвящена изучению проблемы и перспективы развития законодательства об уголовной ответственности за хищения имуществ посредством компьютерной информации, а также рассматриваются отграничения мошенничества с использованием компьютерной информации от смежных составов преступления и пути их преодоления.

В заключении выпускной квалификационной работы автором предложены заслуживающие внимания изменения действующего уголовного законодательства в сфере противодействия рассматриваемым видам преступлений. Оформление работы не вызывает нареканий. Поставленные перед автором цели и задачи достигнуты.

Все это свидетельствует о том, что представленная выпускная квалификационная работа слушателя Якупова Р.Р. может быть допущена к защите и заслуживает положительной оценки.

Научный руководитель:
профессор кафедры уголовного права
доктор юридических наук, профессор М.В. Талан

С отзывом ознакомлен Якупов Р.Р.

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

Рецензия

на выпускную квалификационную работу по теме «Актуальные вопросы квалификации кражи и мошенничества, совершаемые с использованием компьютерной информации», слушателя учебной группы №123 факультета подготовки специалистов по программам высшего образования Казанского юридического института МВД России младшего лейтенанта полиции Якупова Р.Р.

Выпускная квалификационная работа на тему «Актуальные вопросы квалификации кражи и мошенничества, совершаемые с использованием компьютерной информации», подготовленная слушателем факультета очного обучения Казанского юридического института МВД России младшего лейтенанта полиции Якупова Равиля Рамилевича, является актуальной для сотрудников органов внутренних дел Российской Федерации, в связи с тем, что хищения, совершаемые с использованием компьютерной информации в России за последние годы приобрели широкое распространение и имеют тенденцию к росту. На сегодняшний день среди научной литературы, посвященной данной теме, наблюдается малое количество научных исследований, что способствует возникновению множества вопросов квалификаций рассматриваемых преступлений. В связи с этим некоторые вопросы остались дискуссионными, что вызывает потребность в их дополнительном изучении и научной проработке. Противодействие хищениям, совершаемых посредством компьютерной информации стало одной из серьезных проблем, как для отечественных, так и для зарубежных правоохранительных органов.

Структура и содержание работы полностью соответствуют заявленной теме. Структурно выпускная квалификационная работа состоит из введения,

двух глав (Уголовно-правовая характеристика мошенничества в сфере компьютерной информации; Вопросы квалификации преступлений, предусмотренных статьей 159.6 УК РФ и отграничение его от смежных составов), заключения, списка использованных нормативных правовых актов, учебной и учебно-методической литературы.

Во вводной части автор привел обоснование актуальности выбранной темы, поставил перед собой цели исследования и сформулировал задачи по их достижению.

Первая глава посвящена анализу уголовно-правовой характеристике мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ). Рассматриваются особенности систематизации, а также квалификации норм об ответственности за преступления мошенничества в сфере компьютерной информации.

Во второй главе работы изучаются проблемы и перспективы развития законодательства об уголовной ответственности за хищения, совершаемые с использованием компьютерной информации, а также рассматриваются отграничения мошенничества с использованием компьютерной информации от смежных составов преступления и пути их преодоления.

В заключении выпускной квалификационной работы сформулированы выводы и предложения по проведённому научно-практическому исследованию.

Оформление работы не вызывает нареканий. Поставленные перед автором цели и задачи достигнуты. В качестве замечания стоит отметить отсутствие полных статистических данных за период 2016-2017 гг., однако это не снижает общий, несомненно, высокий уровень работы.

Исходя из вышеизложенного стоит отметить, что представленная выпускная квалификационная работа слушателя Якупова Р.Р. может быть допущена к защите и заслуживает оценки «отлично».

Преподаватель кафедры уголовного процесса
майор полиции Д.В. Кузнецов

С отзывом ознакомлен Якупов Р.Р.

Рецензия
на выпускную квалификационную работу по теме «Актуальные вопросы квалификации кражи и мошенничества, совершаемые с использованием компьютерной информации», слушателя учебной группы №123 факультета подготовки специалистов по программам высшего образования Казанского юридического института МВД России младшего лейтенанта полиции Якупова Р.Р.

Выпускная квалификационная работа[1] по теме «Преступления экстремистского характера: теория и практика противодействия», подготовленная слушателем факультета очного обучения[2] Казанского юридического института МВД России[3] младшего лейтенанта полиции Якуповым Равилем Рамилевичем, представляется весьма актуальной для сотрудников органов внутренних дел Российской Федерации[4], поскольку посвящена выработке практических знаний и умений по применению мер предупреждения и противодействия преступлениям совершаемым посредством компьютерной информации.

В современном преступном мире все больше внимания уделяется на преступления, совершаемые посредством компьютерных технологий. Несмотря на постоянное увеличение уровня исследуемых преступлений, их раскрываемость остается на низком уровне, а латентность, наоборот, высокой. Сохраняются также сложности в правоприменительной практике при привлечении к уголовной ответственности по ст.ст. 158, 159.6, 272, 273 УК РФ.

Содержание выпускной квалификационной работы составляют введение, две главы (Уголовно-правовая характеристика мошенничества в сфере компьютерной информации; Вопросы квалификации преступлений, предусмотренных статьей 159.6 УК РФ и отграничение его от смежных составов) заключение, список использованных нормативных правовых актов, учебной и учебно-методической литературы. Положительным моментом является наличие в рукописи работы перечня нормативных документов МВД России по изучаемой тематике.

Следует обратить внимание на стремление автора рассмотреть максимальное количество проблемных вопросов многие, из которых представляют научный интерес, в частности, разграничения таких преступлений как кражи и мошенничества в сфере компьютерной информации.

Выполненная выпускная квалификационная работа, опирается на солидную нормативную, теоретическую и эмпирическую базу. Автор, в принципе, верно, определяет объект и предмет исследования, его цели и задачи, методологию и методику.

Якупов Р.Р. в достаточной мере использует монографическую, периодическую и учебную литературу по рассматриваемой тематике,

---

[1] Далее – «ВКР и (или) работа».
[2] Далее – «ФОО».
[3] Далее – «КЮИ МВД России и (или) институт».
[4] Далее – «Органы внутренних дел» и (или) «ОВД».

современное уголовное законодательство России, также различных периодов его развития, международные акты, законодательства зарубежных стран, опирается на материалы Постановлений Верховного Суда РФ, судебно-следственной практики, статистические данные.

Особого внимания заслуживают конкретные меры предупреждения рассматриваемого преступления. Автором рассмотрены предпосылки широкомасштабного распространения киберпреступности в России. На основе проведенного анализа, с использованием обширных эмпирических и статистических исследований, автором обосновывается необходимость проведения ряда мероприятий по снижению уровня компьютерных преступлений в России.

Научная и практическая значимость работы состоит в том, что выводы, сделанные на основе монографических исследований, обобщения судебно - следственной практики, предложения по квалификации рассматриваемого преступления могут быть использованы как в практической деятельности правоохранительных органов, а также в дальнейших научных исследованиях по рассматриваемой тематике.

Выпускная квалификационная работа Якупова Р.Р. носит самостоятельный характер, написана доступным языком, оформлена в соответствии с установленными требованиями.

Исходя из вышеизложенного стоит отметить, что представленная выпускная квалификационная работа слушателя Якупова Р.Р. может быть допущена к защите и заслуживает положительной оценки.

Консультант,

Заместитель начальника отдела
по расследованию организованной
преступной деятельности в сфере
экономики и коррупции
майор юстиции Хамидуллин Д.Д.

М.П.
«11» 01 2017 г.

с рецензией ознакомлен Якупов Р.Р.