Федеральное государственное казенное образовательное учреждение
высшего образования
«Восточно-Сибирский институт
Министерства внутренних дел Российской Федерации»

Е. Н. Бархатова

ОСОБЕННОСТИ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ ПРОТИВ СОБСТВЕННОСТИ, СОВЕРШАЕМЫХ ПОСРЕДСТВОМ МОБИЛЬНОЙ СВЯЗИ И СЕТИ «ИНТЕРНЕТ»

Учебное пособие

Иркутск
Восточно-Сибирский институт МВД России
2017

УДК 343.3/.7
ББК 67.408.1

Печатается по решению редакционно-издательского совета
ФГКОУ ВО «Восточно-Сибирский институт МВД России»

Рецензенты:
О. М. Шаганова — ст. преподаватель каф. уголовного права и криминологии Барнаульского юридического института МВД России, канд. юрид. наук;
К. Н. Карпов — ст. преподаватель каф. уголовного права Омской академии МВД России, канд. юрид. наук

Бархатова Е. Н. Особенности квалификации преступлений против собственности, совершаемых посредством мобильной связи и сети «Интернет»: учебное пособие / Е. Н. Бархатова. — Иркутск: ФГКОУ ВО ВСИ МВД России, 2017. — 80 с.

В настоящем учебном пособии рассматриваются понятие и общая характеристика преступлений против собственности, совершаемых посредством мобильной связи и информационно-телекоммуникационной сети «Интернет», проводится отграничение составов данных преступлений от смежных составов преступлений, освещаются проблемные вопросы их квалификации.

Предназначено для практических работников, занимающихся расследованием и судебным рассмотрением уголовных дел о преступлениях против собственности, совершаемых посредством мобильной связи и сети «Интернет», преподавателей, адъюнктов, слушателей, курсантов, а также аспирантов, магистрантов и студентов юридических вузов

УДК 343.3/.7
ББК 67.408.1

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Преступления против собственности ежегодно составляют практически половину от общей массы преступлений. Так, в 2012 г. в России зарегистрировано около 1,4 млн преступлений, в 2013 — чуть более 1,3 млн, в 2014 — 1,3 млн, в 2015 — 1,4 млн, в 2016 — 1,2 млн[1]. В Иркутской области в 2016 г. зарегистрировано более 25 тыс. имущественных преступлений (АППГ — 30,7 тыс.; –16,6 %)[2]. Ситуация осложняется тем, что в условиях развития информационных технологий набирает обороты так называемая «киберпреступность». Получили широкое распространение мошенничества, совершаемые посредством мобильной связи и информационно-телекоммуникационной сети «Интернет», с использованием средств платежей. Так, в 2015 г. в России зарегистрировано 196 700 преступлений, ответственность за которые предусмотрена ст.ст. 159—159.6 УК РФ (на 25 % больше аналогичного периода 2014 г. — 160 214). На фоне общего роста числа зарегистрированных мошенничеств наблюдается значительный рост так называемых «компьютерных» мошенничеств, который в 2015 г. составил 447 % (с 995 по итогам 2014 г. до 5 443). Несмотря на незначительное снижение числа таких мошенничеств в 2016 г. (на 20,5 %; до 4329), проблема не теряет своей актуальности. При этом раскрываемость последних по итогам 2015 г. находилась на низком уровне и составляла лишь 7,4 % (в 2014 г. — 32,2 %). По итогам 2016 г. данная негативная тенденция сохранилась. Раскрываемость мошенничеств в сфере компьютерной информации снизилась до 6,6 %. Лидирует по числу данных преступлений Тюменская область (917 фактов), Удмуртская Республика (544), Республика Коми (515)[3].

Существенное снижение числа раскрытых преступлений обусловлено совершенствованием способов посягательств, которым на данный момент органы внутренних дел не готовы противостоять.

Наряду с мошенничеством многочисленны факты краж денежных средств, совершаемых посредством пластиковых карт, сети «Интернет», мобильной связи. Так, в 2016 г. только в Иркутской области зарегистрировано 207 таких фактов (АППГ — 377; –38,6%)[4].

Одним из факторов, повышающих актуальность проблемы противодействия рассматриваемой категории преступлений, является возрастающий

---

[1] Статистические данные МВД России. [Электронный ресурс]. — Режим доступа: http:www.mvd.ru/deyatelnost/statistics (дата обращения: 03.03.2017).

[2] Статистические данные Информационного центра ГУ МВД России по Иркутской области.

[3] Данные ЦСИ ГИАЦ МВД России.

[4] Статистические данные Информационного центра ГУ МВД России по Иркутской области.

размер ущерба, причиняемого ими. Так, ежегодные потери мировой экономики от экономических преступлений, совершаемых в киберпространстве, составляют 500 млрд долл.[1].

Преступления против собственности, совершаемые посредством сети «Интернет» и мобильной связи, вызывают трудности при их квалификации, обусловленные недостаточной осведомлённостью практических сотрудников об отдельных технических особенностях той или иной системы.

Учитывая, что в современном мире человек активно пользуется Интернетом, а также мобильными средствами связи для совершения различного рода платежей — покупок, переводов, оплаты кредитов и коммунальных платежей, можно предположить, что в ближайшие годы, преступления против собственности, совершаемые в киберпространстве, приобретут большую актуальность, нежели кражи и мошенничества в традиционном понимании.

Объектом данного исследования являются отношения собственности, а также отношения, касающиеся нормальной работы с компьютерной информацией.

Целью настоящей работы является выявление особенностей квалификации преступлений против собственности, совершаемых посредством сети «Интернет» и мобильной связи.

Для достижения поставленной цели необходимо решение следующих задач:

— рассмотреть общую характеристику преступлений против собственности, совершаемых посредством мобильной связи и сети «Интернет»;

— выделить признаки, позволяющие отграничить их от преступлений в сфере компьютерной информации;

— рассмотреть теоретические вопросы квалификации рассматриваемой группы преступлений;

— проанализировать судебную практику.

[1] *Простосердов М. А*. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. …канд. юрид. наук. — М., 2016. — С. 3.

Глава 1.
ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ ПРОТИВ СОБСТВЕННОСТИ, СОВЕРШАЕМЫХ ПОСРЕДСТВОМ МОБИЛЬНОЙ СВЯЗИ И СЕТИ «ИНТЕРНЕТ», ИХ ОТЛИЧИЕ ОТ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1. Общая характеристика преступлений против собственности, совершаемых посредством мобильной связи и сети «Интернет»

Представляя собой один из самых ранних видов преступлений, за которые в древнейших источниках права устанавливалась уголовная ответственность, наряду с преступлениями против жизни или здоровья, сегодня посягательства на имущество приобретают качественно новые формы и порождают вопросы относительно своих особенностей. В частности, интерес представляет уголовно-правовая характеристика группы имущественных преступлений, совершаемых посредством мобильной связи и информационно-телекоммуникационной сети «Интернет».

Начиная характеристику с объекта посягательства, стоит указать на то, что он принципиально не отличается от видового объекта преступлений против собственности, каковым следует признавать общественные отношения, возникающие по поводу распределения и перераспределения материальных благ, а именно по поводу владения, пользования или распоряжения ими.

Однако для составов таких преступлений характерен дополнительный объект — общественные отношения, складывающиеся по поводу нормального обмена информацией с помощью средств связи, а также нормального функционирования информационных систем.

Кроме того, в ряде случаев может иметь место факультативный объект. Таковым могут выступать жизнь или здоровье человека, честь и достоинство личности, конституционные права и свободы, здоровье населения и общественная нравственность.

Так, при вымогательстве угроза причинения вреда жизни или здоровью может быть передана посредством электронной почты или в СМС-сообщении. В сети «Интернет» с целью вымогательства могут быть размещены сведения, позорящие потерпевшего, с условием, что после передачи денежных средств преступником будет дано опровержение. В ходе посягательства на имущество, совершаемое посредством информационных технологий, может быть нарушена тайна переписки потерпевшего.

Особого внимания заслуживает предмет рассматриваемой группы преступлений. В первую очередь это, конечно, имущество, к которому следует относить ценности, обладающие экономической значимостью, суще-

ствование которых возможно в цифровой среде. К таковым могут быть отнесены безналичные и электронные денежные средства, криптовалюта.

Безналичные денежные средства представляют собой определённую сумму средств, которая хранится на том или ином виде счёта и используется для расчётов. При расчёте безналичными средствами лишь изменяется запись на конкретных счетах.

Электронные деньги — несколько иная категория. Они представляют собой денежные средства, эмитированные какой-либо организацией, например, любым банком. Наличные же и безналичные деньги эмитируются только Центральным Банком Российской Федерации[1].

Согласно п. 18 ст. 3 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платёжной системе» электронные денежные средства представляют собой денежные средства, которые предварительно предоставлены другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа. При этом не являются электронными денежными средствами денежные средства, полученные организациями, осуществляющими профессиональную деятельность на рынке ценных бумаг, клиринговую деятельность и (или) деятельность по управлению инвестиционными фондами и негосударственными пенсионными фондами и осуществляющими учёт информации о размере предоставляемых денежных средств без открытия банковского счета в соответствии с законодательством, регулирующим деятельность этих организаций. Таким образом, лицо осуществляет пополнение своего «электронного кошелька» (при помощи системы Western Union, банковским переводом, через систему E-Gold и иными способами), а затем может осуществлять расчёты, направляя информацию, определённую совокупность цифровых сигналов по указанному адресу. Отражение указанной информации в «электронном кошельке» продавца будет свидетельствовать о производстве оплаты. Теперь выясним, что из себя представляют организации, о которых идёт речь во второй части рассматриваемого положения.

Итак, согласно определению, данному в ч. 18 ст. 2 Федерального закона от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг» к профессиональным участникам рынка ценных бумаг, относятся брокер, дилер, управляющий, депозитарий, держатели реестра (регистраторы). Как определено в п. 1 ст. 2 Федерального закона от 7 февраля 2011 г. № 7-ФЗ «О клиринге и клиринговой деятельности», клиринг — это определение подлежащих ис-

[1] См.: *Простосердов М. А.* Указ соч. С. 3.

полнению обязательств, возникших из договоров, и подготовка документов, являющихся основанием прекращения или исполнения таких обязательств.

Согласно положениям п. 4 ст. 3, п. 3 ст. 11, п. 1 ст. 38 Федерального закона от 29 ноября 2001 г. № 156-ФЗ «Об инвестиционных фондах», управляющая компания инвестиционного фонда, управляющая компания паевого инвестиционного фонда — это созданное в соответствии с законодательством РФ акционерное общество или общество с ограниченной (дополнительной) ответственностью; инвестиционные резервы акционерного инвестиционного фонда должны быть переданы в доверительное управление управляющей компании, соответствующей требованиям названного закона, за исключением установленного случая; управляющая компания паевым инвестиционным фондом осуществляет доверительное управление паевым инвестиционным фондом путём совершения любых юридических и фактических действий в отношении составляющего его имущества, а также осуществляет все права, удостоверенные ценными бумагами, составляющими паевой инвестиционный фонд, включая право голоса по голосующим ценным бумагам.

Управляющая компания негосударственного пенсионного фонда, согласно ст. 3 Федерального закона от 7 мая 1998 г. № 75-ФЗ «О негосударственных пенсионных фондах» — это акционерное общество, общество с ограниченной (дополнительной) ответственностью, созданные в соответствии с законодательством РФ и имеющие лицензию на осуществление деятельности по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами.

Из определения электронных денежных средств видно, что они обусловлены такой категорией, как «электронные средства платежа», определяемой, в свою очередь, как средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях перевода денежных средств в рамках применяемых форм безналичных расчётов с использованием информационно-телекоммуникационных технологий, электронных носителей информации, в том числе платёжных карт, а также иных технических устройств. На основании обозначенной взаимосвязи и исходя из определения, учёными выявлены юридические условия перехода денежных средств в электронные. К таким условиям относятся: предоставление денежных средств одним лицом другому лицу, учитывающему информацию о размере денежных средств без открытия банковского счета; дача распоряжения по дальнейшему движению денежных средств исключительно с использованием электронных средств платежа; приобретение лицом, учитывающим информацию о размере денежных средств без открытия банковского счёта, юридического статуса оператора электронных денежных средств.

Так, например, в соответствии с положениями Федерального закона от 07.02.2011 № 7-ФЗ «О клиринге и клиринговой деятельности» клиринговые компании вправе открывать как банковский счёт, так и счёт депо

и товарный счёт. На данных счетах могут размещаться как денежные средства, так и иное имущество. Вместе с тем, данные денежные средства не относятся к электронным, поскольку собственник данных средств не может давать клиринговой компании распоряжения по их дальнейшему движению, а клиринговая компания, в свою очередь, не обладает юридическим статусом оператора электронных денежных средств.

Ещё одним средством платежа является криптовалюта, представляющая собой электронный механизм обмена, эмиссию и учёт которого зачастую децентрализованы. Особенность криптовалюты состоит в том, что обменные процессы не регулируются каким-либо внутренним или внешним администратором. В связи с этим банки, а также государственные органы, осуществляющие контроль за совершением транзакций, не могут воздействовать на данные транзакции, это обстоятельство обеспечивает необратимость сделок. Все транзакции совершаются исключительно через доступ к приватному ключу владельца. Эмиссия и учёт криптовалюты основаны на криптографических методах шифрования компьютерной информации. Криптография, т. е. определённые методы шифрования информации, используется не для ограничения доступа к данным о транзакциях, а для гарантирования неизменности цепочки блоков базы транзакций. Это обеспечивает защиту, поскольку изменения в одном блоке цепочки транзакций приведёт к неизбежности внесения изменений в другой блок.

Криптовалюта, по мнению Федеральной службы по финансовому мониторингу Российской Федерации, обладает рядом признаков, таких как децентрализация её эмиссии, анонимность пользователей (все транзакции между всеми «кошельками» общедоступны, но нет привязки адреса к конкретному человеку), отсутствие отчётной документации[1].

В настоящее время криптовалюта активно используется при расчётах и в полной мере может быть отнесена к имуществу, поскольку обладает определённой стоимостью, служит виртуальным эквивалентом материальных ценностей и принадлежит конкретным лицам. Хотя вопрос об отнесении криптовалюты к имуществу в науке уголовного и гражданского права решается неоднозначно, в первую очередь потому, что криптовалюта не подпадает ни под одну категорию из указанных в ст. 128 ГК РФ, согласно которой к объектам гражданских прав относятся вещи, включая наличные деньги и документарные ценные бумаги, иное имущество, в том числе безналичные денежные средства, бездокументарные ценные бумаги, имущественные права; результаты работ и оказание услуг; охраняемые результаты интеллектуальной деятельности и приравнённые к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага. Криптовалюта не является деньгами в том смысле, в котором они понимаются

[1] Информационное сообщение Росфинмониторинга «Об использовании криптовалют» // СПС «КонсультантПлюс».

гражданским правом. Опровергая факт несоответствия криптовалюты требованиям, предъявляемым к имуществу, А. А. Фатьянов предлагает считать её «иным имуществом», указание на которое присутствует в ст. 128 ГК РФ[1].

Перечисленные положения указывают на необходимость учёта всех правовых свойств предмета в их совокупности и позволяют предложить следующее определение чужого имущества: это имущество, не находящееся в собственности или законном владении виновного либо вверенное виновному на время, а также имущество, к которому виновный имеет доступ на законных основаниях, исключая право собственности и владения.

Статьи 159, 159[6] и 163 УК РФ предусматривают право на имущество как предмет преступления. В науке уголовного права существует множество подходов к определению понятия права на имущество[2]. По нашему мнению, этот спор неуместен. Вопрос в данном случае состоит, скорее, в соотношении уголовного и гражданско-правового понятий имущества. Как можно заметить, указанные понятия не совпадают, хотя последнее составляет основу первого.

Следующей категорией, выделенной законодателем в качестве предмета преступлений против собственности, являются другие действия имущественного характера. Данный предмет указан в ст. ст. 163 и 165 УК РФ.

К имущественному действию вообще нужно относить активное поведение лица, направленное на возникновение, изменение или прекращение имущественных отношений[3]. Таким образом, под другими действиями имущественного характера в уголовном праве следует понимать действия, направленные на возникновение, изменение или прекращение имущественных отношений обязательственного характера, в целях получения определённой выгоды. Среди таких действий можно назвать прощение долга; отсрочку или рассрочку платежей; занижение стоимости передаваемого имущества; уменьшение арендных и иных платежей; получение льготных кредитов; снижение процентных ставок за пользование банковскими ссудами; безвозмездное выполнение работ и оказание услуг; безвозмездное использование чужого имущества; получение каких-либо иных имущественных льгот и преимуществ. Перечень подобных действий остаётся открытым. Применительно к составу вымогательства сами действия неуместно назы-

---

[1] *Фатьянов А. А.* Правовой анализ категории «электронные денежные средства» в российском законодательстве // Гражданское общество в России и за рубежом. 2014. № 3 // СПС «Консультант плюс».

[2] *Клепицкий И. А*. Недвижимость как предмет хищения и вымогательства // Госво и право. — 2000. — № 12. — С. 13–15; *Кочои С. М.* Уголовное право. Общая и Особенная части. Краткий курс: учеб. — М., 2010. — С. 209–210; *Питулько К. В.*, *Караковцев В. В.* Уголовное право. Особенная часть. СПб., 2010. С. 111; Уголовное право России. Особенная часть: учеб. / под ред. В. П. Ревина. — М., 2010. — С. 173; *Уголовное право Российской Федерации*. Особенная часть: учеб. / под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. — М., 2009. — С. 168.

[3] *Безверхов А. Г.* Имущественные преступления. — Самара, 2002. — С. 129.

вать предметом, скорее, они будут способом преступления. Предметом же в данном случае выступают выгоды, получаемые злоумышленником в результате названных действий.

Наряду с имуществом, правом на имущество и иными действиями имущественного характера предметом преступлений против собственности, совершаемых посредством сети «Интернет» или мобильной связи следует признать компьютерную информацию.

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

Компьютерная информация сама по себе предметом преступления против собственности чаще всего не является, она служит скорее средством достижения желаемого результата. Вместе с тем, в литературе существует мнение о компьютерной информации как о предмете имущественного посягательства. Так, А. В. Шульга говорит об экономической значимости информации, которая может быть предметом рассматриваемой категории преступлений[1]. А. И. Бойцов называет информацию и информационные продукты стоящими «на грани между понятиями «имущество» и «неимущественное благо»[2].

С позициями указанных авторов следует согласиться лишь в части, учитывая то обстоятельство, что одна лишь экономическая ценность информации отнюдь не делает её предметом имущественного преступления, а в тех случаях, когда информация представляет ценность в виде произведения, программы или иного авторского продукта и похищается, речь следует вести уже не о хищении, а о нарушении авторских прав. Поэтому, если компьютерная информация и может признаваться предметом имущественного преступления, то только такая, которая служит эквивалентом материальных ценностей, соответственно обладает стоимостью, но при этом не является объектом авторского права. К такой информации следует относить электронные деньги и криптовалюту, рассмотренные выше.

Однако, поскольку мы рассматриваем не просто преступления против собственности, а их специфическую группу — совершаемые посредством мобильной связи и сети «Интернет», то следует признать, что компьютерная информация в любом виде будет являться дополнительным объектом данных преступлений, поскольку даже используемая в качестве средства совершения имущественного преступления, она подвергается негативному

---

[1] *Шульга А. В.* Объект и предмет преступления против собственности в условиях рыночных отношений и информационного общества: дис… д-ра. юрид. наук. — Волгоград, 2008. — С. 118–135.

[2] *Бойцов А. И.* Преступления против собственности. — СПб.: Юрид. центр ПРЕСС, 2002. — С. 118.

воздействию со стороны преступника (модификации, удалению, вводу и т. д.).

Таким образом, основным объектом группы преступлений против собственности, совершаемых посредством мобильной связи и сети «Интернет», следует признавать отношения, складывающиеся по поводу распределения и перераспределения материальных благ, влекущие основания для возникновения права пользования, владения или распоряжения имуществом, а дополнительным — нормальное функционирование информационных систем. Предметом указанных преступлений будет являться чужое имущество, в том числе безналичные денежные средства, электронные деньги и криптовалюта.

Объективная сторона рассматриваемой группы заслуживает особого внимания, поскольку зачастую именно по её признакам правоприменитель делает вывод об особенностях субъективной стороны, субъекта, а также в последующем производит квалификацию деяния.

Для объективной стороны рассматриваемой группы преступлений характерно исключительно действие, поскольку обозначенный способ подразумевает реализацию в активной форме, что вытекает из термина «использование». Представляется, что использовать средства связи или Интернет возможно только путём совершения определённых, даже самых минимальных, действий. Прежде всего определим составы преступлений, в которых может иметь место такой способ, как использование средств связи и сети «Интернет». В первую очередь к данной группе относится мошенничество в сфере кредитования (ст. 159^1 УК РФ), мошенничество с использованием платёжных карт (ст. 159^3 УК РФ), мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ), кроме того, к указанным составам следует отнести присвоение или растрату (ст. 160 УК РФ), вымогательство (ст. 163 УК РФ), причинение имущественного ущерба путём обмана или злоупотребления доверием (ст. 165 УК РФ).

Особенностью объективной стороны в данном случае будет способ — «посредством мобильной связи или сети «Интернет». Разберём подробнее указанный способ и его проявления в вышеперечисленных составах преступлений.

Совершение преступлений против собственности посредством мобильной связи возможно в следующих формах:

1. Мошенничество. Мошенничество в свою очередь условно можно разделить на следующие категории:

— контрактное мошенничество — преднамеренное указание неверных данных при заключении контракта или договора;

— хакерское мошенничество — проникновение хакеров в компьютерную систему защиты для удаления механизмов защиты или переконфигурации системы в своих целях;

— техническое мошенничество — неправомочное изготовление телефонных трубок или платёжных телефонных карт с фальшивыми идентификаторами абонентов, номеров и платёжных отметок;

— процедурное мошенничество — неправомочное использование роуминга и других бизнес-процедур (например, биллинга) с целью уменьшения оплаты услуг связи[1];

— мошенничество, реализуемое через звонки с сообщением о том, что карта заблокирована, и собственнику необходимо совершить ряд действий, диктуемых «оператором», а также через СМС-сообщения различного характера (аналогично звонкам о блокировке карты, с просьбой о помощи, связанной с тем, что, к примеру, член семьи попал в беду и т. п.);

— перевод денежных средств со счёта собственника или иного владельца на счёт преступника с помощью услуги «мобильный банк».

К слову, последний вид мошенничества является наиболее распространённым, и вариации его способа многочисленны. Возможны ситуации, когда предварительно совершается кража мобильного устройства, абонентский номер которого привязан к счёту карты собственника. После этого, используя услугу «Мобильный банк», преступник получает возможность осуществить перевод денежных средств со счёта карты собственника на свой счёт. Возможен также вариант, связанный с недобросовестностью операторов сотовой связи. Не секрет, что многие операторы практикуют перепродажу сим-карт, номера которых привязаны к счетам карт бывших владельцев указанных сим-карт. При активации сим-карты её новому владельцу начинают приходить СМС-сообщения от банка (разумеется, в том случае, если прежний владелец сим-карты не сообщил банку о смене абонентского номера), недобросовестный новый владелец сим-карты таким образом получает возможность распоряжаться денежными средствами прежнего её владельца.

Примером такого мошенничества может служить дело С., рассмотренное Братским городским судом Иркутской области. С. тайно похитил мобильный телефон, принадлежащий Ю. Затем, обнаружив, что к сим-карте, находящейся в телефоне, подключена дистанционная финансовая банковская услуга «Мобильный банк» ПАО «Сбербанк России», принял решение о хищении денежных средств со счета банковской карты, принадлежащей Ю.

Реализуя преступный умысел, С. обратился к своему знакомому К. с просьбой помочь ему в осуществлении дистанционного перевода денежных средств с помощью банковской услуги «Мобильный банк» ПАО «Сбербанк России» и передал ему похищенный у потерпевшей сотовый телефон. К., не будучи посвящённым в преступный план С. и полагая, что переданный

[1] *Лопатина Т. М.* Проблемы формирования уголовно-правового способа борьбы с компьютерным мошенничеством // Библиотека криминалиста. — 2013. — № 5. — С. 36.

ему С. сотовый телефон принадлежит С., направил на номер ПАО «Сбербанк России» СМС-сообщение для перевода денежных средств в сумме 7,5 тыс. руб. со счёта банковской карты VISA Classic, принадлежащей потерпевшей, на счёт банковской карты С.

Таким образом, С., при помощи К., путём ввода и модификации компьютерной информации путём незаконного вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации информационно-телекоммуникационных сетей похитил денежные средства в сумме 7,5 тыс. руб., снял со счёта принадлежащей ему банковской карты похищенные денежные средства и распорядился ими по своему усмотрению.

Суд квалифицировал действия С. как кражу (по ч. 1 ст. 158 УК РФ) и мошенничество в сфере компьютерной информации, совершённое с причинением значительного ущерба гражданину (по ч. 2 ст. 159^6 УК РФ)[1].

2. Вымогательство. Совершённым посредством мобильной связи следует считать вымогательство, при котором требование передачи имущества или права на имущество осуществляется в форме СМС-сообщения, при условии, что угроза, подкрепляющая данное требование, воспринимается потерпевшим реально, либо у потерпевшего есть основания ожидать наступления неблагоприятных последствий в случае невыполнения предъявленного требования, даже если оно не подкреплялось угрозой. Кроме того, требование может быть подкреплено угрозой не только словесной, но и в форме демонстрации соответствующих изображений в ММС-сообщениях.

Следующий блок способов касается совершения имущественных преступлений посредством информационно-телекоммуникационной сети «Интернет». Указанные преступления реализуются в следующих формах:

1. Мошенничество в сфере компьютерной информации. Его схемы могут быть самыми разнообразными — от уходящего в прошлое извещения о выигрыше до создания фальшивых интернет-магазинов). Наиболее распространёнными на сегодняшний день являются следующие схемы:

— сверхприбыльные инвестиции — предложение о вложении в высоколиквидные ценные бумаги банков или телекоммуникационных компаний (такие инвестпроекты «гарантируют» безусловный возврат вложенного капитала и высокие прибыли);

— рыночные манипуляции — извлечение прибыли за счёт продажи ценных бумаг, спрос на которые формируется искусственно: манипулятор приобретает бумаги неизвестной реальной компании, затем им распространяется ложная информация об эмитенте, ориентированная на создание повышенного спроса на данные акции и, тем самым, повышение их цены (рост

[1] Приговор Братского городского суда Иркутской области № 1-487/2016 от 08.11.2016 по делу А. [Электронный ресурс]. — Режим доступа: http://www.sudact.ru (дата обращения 30.11.2016).

цен привлекает к акциям интерес индивидуальных инвесторов); дождавшись пиковой цены, мошенники продают свой пакет ценных бумаг по завышенной цене, после сброса на рынок акций их цена возвращается к исходному уровню, в результате мошенники имеют сверхприбыль, а рядовые инвесторы несут убытки;

— фишинг — применяется с целью получения доступа к логину и паролю пользователя; типичными признаками фишинговых писем являются запросы под разными благовидными предлогами о предоставлении личной информации или ложные маркетинговые исследования с просьбой предоставить такую информацию (в качестве примера можно привести фишинг телефонных номеров с последующей подпиской пользователя на платную услугу, с автоматическим продлением без участия пользователя или фарминг, когда злоумышленник распространяет специальные вредоносные программы, которые перенаправляют обращения пользователей к заданным поддельным сайтам);

— подмена данных кода — хищение посредством неверного ввода или вывода в компьютерные системы или из них путём манипуляции программами. Так, начисление заработной платы при известном общем объёме выполненных работ производится раздельно по каждому исполнителю. Подмена шифра настоящего исполнителя шифром заинтересованного нарушителя приведёт к тому, что на счёт мошенника незаконно поступит денежная сумма.

Примером мошенничества в сфере компьютерной информации с использованием возможностей сети «Интернет» можно признать действия гр-ки А., которая совершила хищение денежных средств по следующей схеме. Воспользовавшись своим служебным положением главного бухгалтера сельскохозяйственного промышленного комплекса (далее — СПК), дающим ей полномочия на взаимодействие с финансово-кредитными организациями от имени представляемой организации, действуя в тайне от председателя СПК, имея умысел на хищение денежных средств с расчётного банковского счета СПК, с целью противоправного обогащения, в офисе ОАО «Сбербанк России», не уведомляя работников офиса о своих преступных намерениях, обратилась с заявлением о присоединении к условиям предоставления услуг с использованием системы дистанционного банковского обслуживания в указанной финансово-кредитной организации от имени председателя СПК для организации обслуживания банковского расчётного счета СПК, открытого в названном банке, с использованием системы «Сбербанк Бизнес-онлайн», предоставляющую возможность посредством электронной сети «Интернет» подготавливать и получать платёжные документы и получать информацию о движении денежных средств по счетам, с подключением услуги по расчётно-кассовому обслуживанию в валюте РФ с предоставлением доступа к такой услуге, с указанием абонентского номера телефона для оправки

СМС-паролей и голосовой связи. Указанную процедуру А. выполнила путём обмана, потому как ввела работников банка в заблуждение относительно необходимости кооператива в предоставлении названной услуги, а также подделала подпись председателя СПК на бланке заявления. Кроме того, указывая в заявлении номер телефона как абонентский номер председателя СПК, с целью совершать хищения средств в тайне от последнего, А. указала принадлежащий ей номер. По заявлению А. банком услуга была предоставлена. А. получила возможность дистанционно распоряжаться средствами через одноразовые СМС-пароли на вышеуказанные телефонные номера. Далее А., достоверно зная, что она не обладает правом пользования и распоряжения средствами СПК при помощи системы «Сбербанк Бизнес-онлайн» создавала в форме электронных документов платёжные поручения о переводе денежных средств с банковского расчётного счета СПК на принадлежащий ей расчётный счёт. При выполнении вышеуказанных операций А. получала из банка одноразовые СМС-пароли для подтверждения операций по электронным платёжным поручениям, вводила поступающие пароли, чем выполняла процедуру альтернативного средства подписания платёжных поручений ею как главным бухгалтером кооператива и от имени А., т. е. вводила несанкционированно полученную ею компьютерную информацию, которая ей стала доступна путём обмана сотрудников банка. Созданные платёжные поручения, используя ту же систему, персональный компьютер и сеть «Интернет», А. отправляла в банк по месту открытия расчётного счёта СПК и получила реальную возможность распоряжаться переведёнными в этот период банком на её счёт денежными средствами кооператива на общую сумму 300 000 руб. После поступления денежных средств на принадлежащий ей расчётный счёт А. их обналичивала в банкоматах и оплачивала покупки по безналичному расчёту в торговых сетях, т. е. тратила похищенные средства на личные нужды. Тем самым А. с корыстной целью, противоправно, путём ввода компьютерной информации, а также вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационной сети «Интернет» безвозмездно изъяла и обратила в свою пользу чужое имущество, причинив СПК материальный ущерб в размере 300 000 руб.[1].

2. Вымогательство. Аналогично «мобильному» «сетевое» вымогательство осуществляется путём предъявления требования, но уже через направление угроз на электронную почту потерпевшего. Показательно в этом отношении уголовное дело № 1-343, рассмотренное Ангарским городским судом Иркутской области. П. совершил преступления, предусмотренные п. «б» ч. 3 ст. 163, ч. 1 ст. 183, ч. 3 ст. 30, ч. 2 ст. 183, ч. 1 ст. 272 УК РФ, т. е. осуществил

[1] Приговор Знаменского районного суда Омской области № 1-35/2016 от 03.11.2016 по делу А. [Электронный ресурс]. — Режим доступа: http://www.sudact.ru (дата обращения 30.11.2016).

неправомерный доступ к компьютерной информации ЗАО «Теле-Росс-Тюмень», повлёкший копирование информации о базе данных абонентов «Теле-Росс-Тюмень», его служебно-технической документации, а также сведений бухгалтерского и финансово-отчётного характера, составляющие коммерческую тайну, путём хищения компьютерной информации, а равно иным незаконным способом в целях незаконного использования этих сведений, требовал передачу права на имущество под угрозой распространения сведений, которые могут причинить существенный вред правам или законным интересам ЗАО «Теле-Росс-Тюмень», в лице генерального директора Н., покушался на незаконное разглашение сведений, составляющих коммерческую тайну, без согласия их владельца, совершённое из корыстной заинтересованности. При этом преступление не было доведено до конца по не зависящим от П. обстоятельствам[1].

3. Причинение имущественного ущерба путём обмана или злоупотребления доверием может иметь место в тех случаях, когда, проникая в компьютерную систему, преступник стирает часть данных, либо изменяет эти данные с целью причинить имущественный ущерб потерпевшему. При этом преступник нередко проникает в систему правомерно, с ведома собственника, однако же злоупотребляет доверием последнего либо обманывает его относительно тех манипуляций, которые производятся им с информацией.

Примером причинения имущественного ущерба путём обмана, совершённого посредством сети «Интернет», является приговор Можгинского районного суда Удмуртской Республики по делу М., который, создав вредоносную компьютерную программу, с её помощью осуществлял неправомерный доступ к компьютерной информации — логинам и паролям иных лиц. В последующем М. использовал указанные логины и пароли для неправомерного доступа в Интернет, чем причинял владельцам паролей и логинов имущественный ущерб, поскольку оплата за доступ к сети осуществлялась со счетов последних[2].

К хищению предметов, имеющих особую ценность, применимо то же правило, что и для подобных преступлений, совершаемых с помощью средств мобильной связи.

Необходимо отметить, что в любом из указанных случаев реализация способа совершения преступления происходит с помощью манипуляций с компьютерной информацией. Такими манипуляциями являются ввод, модификация, блокирование, удаление компьютерной информации и вмеша-

---

[1] *Евдокимов К. Н.* Проблемы квалификации и предупреждения компьютерных преступлений: монография. — Иркутск: Ирк. юрид. ин-т (филиал) Академии Ген. прокуратуры РФ, 2009. — С. 96–97.

[2] Приговор Можгинского районного суда Удмуртской Республики № 1-162/2010 от 13.08.2010 по делу М. [Электронный ресурс]. — Режим доступа: http://sudact.ru/regular/doc/8h4NgygCHCUR/ (дата обращения 02.12.2016).

тельство в функционирование средств хранения, обработки и передачи информации, а также информационно-телекоммуникационных сетей. Данные способы включают в себя взлом паролей, кражу номеров кредитных карточек и других банковских реквизитов. Преступник умышленно с целью хищения обманным путём имущества потерпевшего осуществляет доступ к защищённой информации, не имея на это правомочий.

Так, к примеру, Каспийским городским судом Республики Дагестан привлечён к уголовной ответственности по ч. 2 ст. 159.6 УК РФ гр. И., который, с использованием персонального компьютера, подключённого к сети «Интернет» с принадлежащего гр. Р. электронного счёта в системе «Единый кошелёк» путём перечисления на счёт платёжной системы «Киви-кошелёк» похитил денежные средства в сумме 5 тыс. 560 руб. 60 коп., после чего перечислил данную сумму на свой банковский счёт в ОАО «Экспресс-банк» и обналичил посредством снятия через банкомат. Своими действиями гр. И. причинил потерпевшему Р. значительный ущерб на сумму 5 тыс. 560 руб. 60 коп.[1].

Нижегородским городским судом гр. Л. привлечена к уголовной ответственности по ч. 3 ст. 159.6. У Л., работавшей в филиале банка в должности старшего специалиста отдела по работе с корпоративными клиентами, в июне 2012 г. 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 расчётов Marti и затем перечислила указанные денежные средства на имеющиеся у неё банковские карты при помощи сервиса «Лёгкий платёж». Далее Л. по несуществующим анкетным данным создала несколько лицевых счетов на имя Б. и Ж. Согласно условиям работы сервиса «Лёгкий платёж» для осуществления перевода денежных средств с абонентом, т. е. с физическим лицом, должен быть заключён абонентский договор, в соответствии с которым максимальная сумма одной операции по абонентскому номеру составляет не более 14 999 руб., максимальная общая сумма платежей в сутки составляет не более 30 000 руб. 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 проводить большее количество операций. Всего Л. по лицевому счёту 1 на имя Б. произведено 24 опе-

[1] Приговор Каспийского городского суда Республики Дагестан № 1-87/2015 от 12.05.2015 по делу Р. [Электронный ресурс]. — Режим доступа:http://www.sudrf.ru (дата обращения: 15.10.2016).

рации по замене абонентского номера, по лицевому счёту 1 на имя Ж. — 31, по лицевому счёту 2 на имя Б. — 14, по лицевому счёту на имя Ж. — 21[1].

Таким образом, в период с июня по ноябрь 2012 г. с лицевых счетов ключевых клиентов Л. похитила путём переноса на лицевые счета на имя Б. и Ж. денежные средства на общую сумму 2 613 581 руб. 73 коп. Продолжая реализовывать свой преступный умысел, направленный на хищение денежных средств, принадлежащих после проведения операций по переносу денежных средств, Л. провела финансовые корректировки на счетах ключевых клиентов, мотивировав это тем, что был применён 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 неё банковские карты и использовала их по собственному усмотрению.

Помимо способа совершения указанных преступлений особое внимание следует уделить и месту их совершения. По общему правилу таковым стоит признать то место, в котором преступником осуществлялся ввод, модификация, удаление или блокирование компьютерной информации. Однако не все представители науки уголовного права готовы согласиться с данным утверждением. Существует позиция, согласно которой местом совершения преступлений в сфере компьютерной информации, в том числе имущественных, следует признавать киберпространство[2]. Согласно проекту Концепции стратегии кибербезопасности Российской Федерации, разработанной ещё в 2011 г., но так и оставшейся в статусе несогласованного проекта, киберпространство — это сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов сети «Интернет» и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)[3].

В свою очередь, под информационным пространством разработчики проекта понимают сферу деятельности, связанную с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общест-

---

[1] Приговор Нижегородского городского суда № 1-29/2015 от 10.09.2015 по делу А. [Электронный ресурс]. — Режим доступа: http://www.sudact.ru (дата обращения 15.10.2016).

[2] См.: *Киселёв А. К.* Киберпреступность — взгляд из Европы. // Библиотека криминалиста. — 2013. — № 5 (10). — С. 310; *Дашян М. С.* Право информационных магистралей: вопрос правового регулирования в сети «Интернет». М.: Волтерс Клувер, 2007. — С. 81.

[3] *Концепция Стратегии кибербезопасности Российской Федерации*. [Электронный ресурс]. — Режим доступа: http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 01.12.2016).

венное сознание, информационную инфраструктуру и собственно информацию. В связи с этим справедлив взгляд М. А. Простосердова на киберпространство как на искусственно созданную среду, существование которой ограничено информационно-телекоммуникационной сетью, пользователи которой могут свободно вступать в административные, гражданские, уголовные и другие правоотношения[1].

Принятая 5 декабря 2016 г. Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 № 646) предлагает понятие информационной сферы, под которой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Отчасти взгляд на киберпространство как на место совершения преступления возможно признать справедливым. Вместе с тем, такая позиция существенно расходится с традиционным пониманием места преступления, которое непременно должно существовать в объективной реальности, хотя бы потому, что в том числе по территориальности определяется подследственность уголовных дел, и в принципе система правоохранительных органов существует не в виртуальной реальности, а в объективной. При этом даже если признавать киберпространство местом совершения преступления, данный факт никоим образом не сможет повлиять на квалификацию содеянного, а также на установление конкретного места, поскольку киберпространство существует на мировом уровне. В любом случае необходимо будет установить IP-адрес, с которого направлялось то или иное сообщение, или MAC-адрес соответствующего устройства, с которого осуществлялся доступ (ноутбук, планшет, смартфон и т. д.). Указанные адреса привязаны к вещам материального мира (техническим устройствам), поэтому определение места преступления практически не составляет труда.

Таким образом, объективная сторона преступлений против собственности, совершаемых посредством мобильной связи и сети «Интернет», всегда выражается в форме действия, характеризуется специфическим способом — воздействием на компьютерную информацию в целях хищения имущества или причинения имущественного ущерба, а также местом совершения преступления.

Составы преступлений исследуемой группы по способу конструкции объективной стороны в большинстве своём материальны, предполагается наступление последствий в виде хищения имущества или причинения иму-

[1] *Простосердов М. А.* Указ. соч. С. 22.

щественного ущерба. Исключение составляет вымогательство, состав которого является формальным, и преступление считается оконченным с момента предъявления требования.

Субъективная сторона имущественных преступлений, совершаемых посредством сети «Интернет» или мобильной связи выражается в форме прямого умысла. Причём умысел в большинстве случаев является заранее обдуманным. Как справедливо заявляют А. Н. Косенков и Г. А. Чёрный, «хотя киберпространство и является многогранным социальным пространством, в то же время оно остаётся искусственно созданной программно-аппаратной средой, деятельность в которой всё-таки ограничена техническими рамками, что делает предсказуемыми последствия действий. Это, в свою очередь, позволяет злоумышленнику не ощущать неопределённости ситуации, планировать свои действия даже при неблагоприятных для него обстоятельствах, а значит, чувствовать себя более уверенно и спокойно во время совершения преступления»[1]. Преступник готовится заранее к совершению преступления, с этой целью он анализирует финансовое состояние компаний, если речь идёт о списании средств со счетов таких компаний, изготавливает фальшивые документы (платёжные поручения, как было продемонстрировано на примере с бухгалтером СПК), похищает телефон (пример с использованием услуги «Мобильный банк») и т. п. Необходимо отметить, что некоторые подготовительные действия могут образовывать самостоятельные составы преступлений. К примеру, приобретение компьютерных программ, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации образует состав преступления, предусмотренный ст. 273 УК РФ, поэтому хищение денежных средств, совершённое путём модификации компьютерной информации, совершённой с использованием вредоносных программ, будет квалифицироваться по совокупности статей 159[6], 272 и 273 УК РФ. Примером тому может служить приговор Советского районного суда г. Улан-Удэ по делу Б., который приобрёл путём копирования на накопитель на жёстких магнитных дисках своего персонального компьютера, программы, заведомо приводящие к несанкционированному доступу, уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ или их сети без ведома пользователя. После этого Б. с целью блокирования и модификации охраняемой законом компьютерной информации, при помощи своего персонального компьютера, подключённого к сети «Интернет», осуществил использование данных вредоносных компьютерных программ, отправив на адрес электронной почты индивидуального предпринимателя Э., используемый финансовой деятельности, письмо свободного содержания, в которое под видом документа вложил указанные вредоносные

[1] *Косенков А. Н., Чёрный Г. А.* Общая характеристика психологии киберпреступника // Криминол. журнал БГУЭП. — 2012. — № 3 (21). — С. 90.

программы. Продавец-консультант индивидуального предпринимателя Э., не подозревая о вредоносном содержании письма, используя служебный компьютер, открыла данное письмо, тем самым автоматически установив на компьютер вредоносную программу. В результате Б. получил неправомерный доступ к компьютеру индивидуального предпринимателя Э. Получив возможность воспользоваться и ознакомиться с компьютерной информацией, в том числе информацией о банковском счёте и находящимися на нём денежными средствами, Б. зашёл в соответствующую программу и, введя в специальную графу свой абонентский номер сотового оператора, осуществил денежный перевод со счёта Э. на свой собственный, причинив таким образом значительный ущерб потерпевшему. Действия Б. квалифицированы по ч. 2 ст. 273, ч. 2 ст. 272, ч. 2 ст. 159^{6} УК РФ[1].

Вместе с тем не исключено совершение преступления и с внезапно возникшим умыслом. Так, в случае, когда лицо имело умысел лишь на хищение компьютерной информации, т. е. на совершение преступления, предусмотренного ст. 272 УК РФ, но в ходе противоправных действий обнаруживает возможность хищения денежных средств и совершает это хищение, то умысел по отношению к последнему будет являться внезапно возникшим. Кроме того, вопрос об умысле относительно посягательства на нормальное функционирование информационных систем нельзя решить однозначно. Состав преступления, предусмотренного ст. 272 УК РФ, по способу конструкции объективной стороны является материальным, в диспозиции чётко прописаны последствия. Если лицо осуществляет неправомерные действия с конкретной целью совершить хищение или причинить имущественный ущерб, то по отношению к преступлению в сфере компьютерной информации характерно наличие косвенного умысла, потому как лицо предвидит наступление возможных последствий в виде уничтожения, блокирования, модификации или копирования компьютерной информации, не желает, но сознательно допускает наступление таких последствий. Однако такая ситуация весьма абстрактна. В реальности без наступления указанных последствий невозможна дальнейшая реализация действий, направленных на хищение или причинение имущественного ущерба. Даже запоминание лицом конкретной информации, к которой он неправомерно получил доступ, по сути, является копированием, т. к. осуществляется для дальнейшего использования (например, запоминание пароля). Поэтому лицо, осуществляя неправомерный доступ к компьютерной информации, в таком случае желает наступления последствий в виде, например, копирования информации, т. е. действует с прямым умыслом.

[1] Приговор Советского районного суда г. Улан-Удэ (Республика Бурятия) № 1-715/2015 от 22.09.2015 по делу Б. [Электронный ресурс]. — Режим доступа: http://sudact.ru/regular/doc/x60NkKWhBNx3 (дата обращения 01.12.2016).

Особое место в составе субъективной стороны занимают мотив и цель совершения указанных преступлений.

Целью преступлений рассматриваемой категории может выступать завладение имуществом (чаще всего денежными средствами) либо причинение имущественного ущерба. Мотивом выступает корысть. Однако наряду с корыстью среди мотивов посягательств на собственность, совершаемых посредством мобильной связи или сети «Интернет», может быть названа месть. Так, логично, что для причинения имущественного ущерба нехарактерен корыстный мотив. Преступник осуществляет подобные действия скорее с целью отомстить. По некоторым подсчётам по мотиву мести совершается 12,9 % всех компьютерных преступлений[1]. Так, подлежащая увольнению по сокращению штатов из городского управления жилищно-коммунальных услуг г. Курчатова Г., недовольная этим фактом, решила осложнить работу подразделений городской администрации. Используя своё служебное положение, Г., занимавшая должность инженера-программиста, под разными предлогами получила доступ к компьютерам пяти ЖЭУ города и уничтожила содержавшуюся на них программу «Квартплата»[2].

Субъектом преступлений против собственности, совершаемых посредством мобильной связи или сети «Интернет», выступает физическое, вменяемое лицо, достигшее возраста уголовной ответственности. Для перечисленных составов преступлений установлен возраст уголовной ответственности — с шестнадцати лет, за исключением вымогательства, ответственность за которое наступает с четырнадцати лет. Специфическими особенностями субъект преступлений рассматриваемой группы не обладает.

Подводя итог первого параграфа, необходимо акцентировать внимание на следующих положениях:

— основным объектом группы преступлений против собственности, совершаемых посредством мобильной связи и сети «Интернет», следует признавать отношения, складывающиеся по поводу распределения и перераспределения материальных благ, влекущие основания для возникновения права пользования, владения или распоряжения имуществом, а дополнительным — нормальное функционирование информационных систем; предметом указанных преступлений будет являться чужое имущество, в том числе безналичные денежные средства, электронные деньги и криптовалюта;

— объективная сторона преступлений против собственности, совершаемых посредством мобильной связи и сети «Интернет», всегда выражается в форме действия, характеризуется специфическим способом — воздействием на компьютерную информацию в целях хищения имущества или

[1] *Батурин Ю. М.* Компьютерная преступность и компьютерная безопасность. — М.: Юриспруденция, 2015. — С. 102.

[2] Там же. С. 102.

причинения имущественного ущерба, а также местом совершения преступления; указанные преступления могут быть совершены как единолично, так и в соучастии; по способу конструкции объективной стороны составы данных преступлений являются преимущественно материальными, за исключением вымогательства;

— субъективная сторона посягательств на собственность, совершаемых посредством мобильной связи или сети «Интернет», выражена в форме прямого умысла, в ряде случаев по отношению к последствиям в виде уничтожения, блокирования, модификации либо копирования компьютерной информации возможен как прямой, так и косвенный умысел;

— субъект указанной категории преступлений общий, для субъекта вымогательства установлен пониженный возраст уголовной ответственности — с 14-ти лет.

2. Разграничение преступлений против собственности, совершаемых посредством мобильной связи и сети «Интернет», и преступлений в сфере компьютерной информации

В настоящее время информационные системы, облачные технологии охватили практически все сферы жизни граждан. Онлайн-услуги, интернет-магазины набирают всё большую популярность и довольно успешно конкурируют с реальными магазинами, а тем более офисами и расчётными центрами, куда граждане ввиду экономии времени обращаются с каждым годом всё реже.

Перевод имущественных отношений в интернет-пространство способствует появлению и распространению имущественных киберпреступлений. Однако тесное переплетение посягательств на имущество с уголовно наказуемыми деяниями в сфере компьютерной информации нередко провоцирует ошибки в квалификации. С одной стороны, необходимо учитывать оба факта: и посягательство на имущество, и нарушение нормального обмена компьютерной информацией и её использования. С другой стороны, необходимо учитывать, что в подобном случае не исключена возможность двойного вменения, что недопустимо.

В связи с указанными обстоятельствами важно уделить особое внимание вопросам отграничения преступлений против собственности, совершённых с помощью информационных систем, от преступлений в сфере компьютерной информации.

Руководствуясь правилами квалификации преступлений, начнём отграничение с объективной стороны.

Особенностью объективной стороны рассматриваемой категории преступлений выступает способ. Ввиду инновационности способа совершения преступлений порождаются не только многочисленные вопросы их раскрытия и расследования (сбора доказательственной базы, реализации результатов оперативно-розыскных мероприятий и т. д.), но, в первую очередь, вопросы квалификации и отграничения от смежных составов преступлений.

Разумеется, если речь идёт о мобильной связи и сети «Интернет», где находит своё отражение компьютерная информация, основными составами, граничащими с составами преступлений рассматриваемой группы, будут являться преступления в сфере компьютерной информации.

Объективная сторона исследуемых групп преступлений достаточно схожа. Воздействие на компьютерную информацию происходит как собственно в целях неправомерного доступа к ней, так и с целью совершения преступления против собственности. Вместе с тем, если в первом случае воздействие на компьютерную информацию выступает в роли собственно деяния, то во втором указанное воздействие является средством совершения преступления. Неправомерный доступ к компьютерной информации либо создание и использование вредоносных компьютерных программ, нарушение правил эксплуатации средств хранения информации, являясь самостоятельными преступлениями, при совершении преступлений против собственности выступают в качестве подготовительных действий. Таким образом, если лицо совершило, к примеру, неправомерный доступ к компьютерной информации с целью приготовления к совершению преступления против собственности, но, по не зависящим от него обстоятельствам не смогло совершить посягательство на имущество (например, хакерская атака была выявлена сотрудниками правоохранительных органов), его действия следует квалифицировать по ст. 272 УК РФ, а также (при наличии умысла и при условии, что преступление относится к категории тяжких), по ч. 1 ст. 30 и ч. 3 или ч. 4 ст. 159^{6} УК РФ. Подобной точки зрения придерживаются и суды. Так, в обзоре судебной практики по делам о мошенничестве, присвоении и растрате Пензенского областного суда указано, что, если не наступили последствия в виде материального ущерба собственнику или иному обладателю имущества по причинам, не зависящим от воли виновного при совершении мошенничества путём воздействия на компьютерную информацию, его действия следует квалифицировать как покушение на данное преступление и по совокупности с действиями, ответственность за которые предусмотрена ст. 272 или 273 УК РФ[1]. По данным ФСБ России на кредитные организации страны ежедневно совершаются кибератаки с целью завладения денежными средствами, находящимися на их счетах, однако,

[1] Обзор практики рассмотрения уголовных дел о мошенничестве, присвоении и растрате (статьи 159, 159.1—159.6, 160 УК РФ) судами Пензенской области в 2014—2015 гг. [Электронный ресурс]. — Режим доступа: http://www.oblsud.penza.ru/item/1220/ (дата обращения: 09.12.2016).

в большинстве случаев системы безопасности банков обеспечивают защиту операций. К примеру, в 2016 г. Сбербанк России обращался в правоохранительные органы по поводу мощных DDoS-атак, которые велись из разных стран, но координировались из одной точки[1].

Вместе с тем, при совершении преступлений против собственности доступ к компьютерной информации может осуществляться и правомерно, однако действия, производимые с данной информацией, будут противоправными. Показателен приговор в отношении М., вынесенный Железнодорожным районным судом г. Читы Забайкальского края. М. приобрела сим-карту для личного пользования. К данной сим-карте ошибочно была подключена услуга «Мобильный банк» (возможно номер указанной карты ранее использовался иным владельцем). М. при активации указанной сим-карты получила смс-оповещение о перечислении на счёт К. 10000 руб. У М. возник умысел на хищение указанных денежных средств, который был ею реализован[2]. В данном случае М., являясь собственником сим-карты, имела правомерный доступ ко всей информации, содержащейся в телефоне и поступающей на принадлежащий ей абонентский номер, однако неправомерно воспользовалась указанной информацией, в связи с чем суд справедливо квалифицировал её действия лишь по ч. 2 ст. 159^6 УК РФ.

Иная ситуация имеет место в случае якобы правомерного, на первый взгляд, доступа к компьютерной информации.

Так, Шелеховским городским судом Иркутской области А. осуждена по ст. 159^6 УК РФ за совершение преступления при следующих обстоятельствах. А. в палате больницы похитила паспорт гражданина РФ на имя К., после чего в отделении офиса банка представилась данными К. и, предъявив паспорт гражданина РФ на имя К., обратилась с заявлением о выдаче ей международной дебетовой карты «Visa Electron Momentum» для своего личного пользования, заполнив и подписав заявление на банковское обслуживание, заявление на получение международной дебетовой карты Сбербанка России, подделав подпись К. на всех документах, получила вышеуказанную международную дебетовую карту и стала пользоваться как своей. При этом А. подключила к данной карте услуги «Мобильный банк», «Сбербанк-онлайн», получив постоянный идентификатор и пароль для пользования. В ходе использования данной карты, А. посредством услуги «Сбербанк-онлайн» зашла в личный кабинет К., где отражаются все сведения о счетах и наличии на них денежных средств последней. Увидев, что на счёте у К. имеются денежные средства в сумме 610 тыс. руб., решила перевести 600 тыс. руб. на свой счёт. После этого А. обналичила часть денежных средств в сумме

[1] Киберпонедельник. [Электронный ресурс]. — Режим доступа: http://news.rambler.ru/business/35481716-5-dekabrya-chernyy-ponedelnik/ (дата обращения 05.12.2016).

[2] Приговор Железнодорожного районного суда г. Читы (Забайкальский край) № 1-166/2016 от 22.04.2016 по делу Г. [Электронный ресурс]. — Режим доступа: http://sudact.ru/regular/doc/qVBsoHNvRYrQ/ (дата обращения: 06.12.2016).

40 тыс. руб., затем — в сумме 50 тыс. руб. Затем А. вернула на банковский счёт К. посредством услуги «Сбербанк-онлайн» 200 тыс. руб.[1].

В данном случае виновная решила «не брать лишнего» и вернуть часть денег, в которых, по-видимому, не испытывала необходимости, их законной владелице. Вместе с тем данный факт ни в коем случае не оправдывает виновную и может служить лишь смягчающим обстоятельством, в случае полного возмещения нанесённого ущерба, в соответствии со ст. 61 УК РФ.

Интересно, что в данном случае суд не посчитал необходимым дополнительно квалифицировать содеянное по ст. 272 УК РФ. Такая позиция вызывает сомнения ввиду наличия факта неправомерного доступа к компьютерной информации, более того, повлёкшего её изменение. Ведь А. получила доступ к информации о счетах К. путём обмана сотрудника банка, оформлявшего дебетовую карту, следовательно — неправомерно. Более того, А. совершила действия по изменению информации, к которой неправомерно получила доступ, с целью собственного обогащения. Таким образом, фактически имеет место состав преступления, предусмотренный ч. 2 ст. 272 УК РФ, т. е. неправомерный доступ к компьютерной информации, совершённый из корыстной заинтересованности. Поэтому позиция суда представляется весьма спорной.

Основная проблема разграничения преступлений против собственности и преступлений в сфере компьютерной информации заключается в том, что в обоих случаях объектом посягательства является нормальный обмен компьютерной информацией. Отличие в данном случае — характер объекта, его вид. Следует подчеркнуть, что для рассматриваемой категории преступлений нормальный обмен компьютерной информацией характерен именно в качестве дополнительного, а не факультативного объекта, поскольку имеет место в любом случае. Более того, следует отметить, что для мошенничества в сфере компьютерной информации дополнительный объект в виде нормального обмена компьютерной информацией также будет иметь место в любом случае, исходя уже из диспозиции ст. 159^6 УК РФ.

Так, к примеру, Братским районным судом Иркутской области Г. осуждена по ч. 2 ст. 159^6 и ч. 2 ст. 272 УК РФ за совершение неправомерного доступа к компьютерной информации с корыстной целью и последующего совершения мошенничества в сфере компьютерной информации, чем причинила значительный ущерб потерпевшему. Г., используя услугу «Мобильный банк» с номера лицевого счета потерпевшего перевела на свой лицевой счёт денежные средства[2]. Таким образом, основной целью Г. являлось

[1] Приговор Шелеховского городского суда Иркутской области от 10.02.2015 № 1-12/2015 по делу А. [Электронный ресурс]. — Режим доступа: http://sudact.ru (дата обращения 06.03.2017).

[2] Приговор Братского районного суда Иркутской области № 1-122/2015 от 15.05.2015 по делу Г. [Электронный ресурс]. — Режим доступа: http://sudact.ru/regular/doc/qVBsoHNvRYrQ/ (дата обращения 06.12.2016).

завладение денежными средствами, т. е. основным непосредственным объектом выступают отношения собственности. Нормальный обмен компьютерной информацией, заключающийся в правомерном направлении собственником денежных средств СМС-сообщений оператору соответствующей финансовой организации, уполномочивающих данного оператора производить конкретные операции с указанными средствами, в частности их списание на лицевой счёт иного лица, в рассматриваемом случае нарушен. Во-первых, Г. воспользовалась мобильным устройством, не принадлежащим ей, не имея на то соответствующего права. Во-вторых, осуществила неправомерное вмешательство в компьютерную систему — не имея правомочий на рассылку от имени собственника распорядительных СМС-сообщений, создала такое сообщение и направила его оператору финансовой организации. В связи с этим Г. осуществила посягательство на дополнительный объект — нормальный обмен компьютерной информацией. Вместе с тем, сравнение санкций ст. 272 УК РФ и ст. 159.6 УК РФ показывает, что неправомерный доступ является более общественно опасным преступлением. Следовательно, неправомерный доступ, выступающий способом совершения мошенничества, требует дополнительной квалификации по ст. 272 УК РФ[1].

Очевидное отличие составов преступлений против собственности, совершаемых посредством мобильной связи или сети «Интернет», от компьютерных преступлений, состоит в предмете посягательства. В первом случае предметом выступают денежные средства и иное имущество, а во втором — компьютерная информация. Следует также учитывать тот факт, что компьютерная информация при совершении преступления против собственности скорее будет относиться к средству совершения преступления.

Субъективная сторона двух рассматриваемых групп отличается преимущественно целью. Для преступлений против собственности характерна цель завладения имуществом или причинения имущественного ущерба, для компьютерных преступлений цель может быть самой разнообразной: получение сведений, составляющих государственную или коммерческую тайну, плагиат, уничтожение важной для потерпевшего компьютерной информации из желания отомстить или по другой причине и т. п.

Особую роль в субъективной стороне рассматриваемых преступлений играет мотив. Для посягательств на имущество характерен корыстный мотив, для компьютерных преступлений возможно наличие любого мотива (мести, хулиганских побуждений, вражды и пр.). Однако не стоит забывать о том, что в статьях 272 и 273 УК РФ предусмотрен квалифицирующий признак «совершённое из корыстной заинтересованности». И. А. Клепицкий определяет корыстную заинтересованность как мотивацию, направленную

[1] *Болсуновская Л. М.* Мошенничество в сфере компьютерной информации: анализ судеб. практики // Угол. право. — 2016. — № 2. — С. 16.

на извлечение какой-либо имущественной (исчисляемой деньгами) выгоды для себя или другого лица[1]. В таком случае возникает вопрос о том, каким образом отграничивать мошенничество в сфере компьютерной информации от неправомерного доступа к компьютерной информации, совершённого из корыстной заинтересованности. И. А. Клепицкий, принимая ст. 159[6] УК РФ за специальную норму по отношению к ст. 272 УК РФ, указывает, что при наличии в содеянном всех признаков мошенничества в сфере компьютерной информации содеянное квалифицируется по ст. 159[6] УК РФ и дополнительная квалификация по ст. 272 УК РФ не требуется[2].

Так, например, Братским городским судом Иркутской области С. был осуждён по ст. 159[6] УК РФ и ст. 272 УК РФ за совершение преступлений при следующих обстоятельствах.

С., введя в заблуждение А., попросил якобы для осуществления звонка сотовый телефон. Воспользовавшись отсутствием внимания со стороны А., С. просмотрел журнал СМС-оповещений, в котором увидел СМС-оповещения о выполнении финансовых транзакций по счёту банковской карты, принадлежащей А., убедился в возможности совершения хищения денежных средств, принадлежащих А., со счёта его банковской карты путём использования подключённой дистанционной финансовой банковской услуги. Направив СМС-запрос на соответствующий номер банковской услуги С. перевёл деньги со счёта А. на иные банковские счета, оплатив различные товары и услуги[3].

В данном случае основной целью С. было получение имущественной выгоды в виде завладения денежными средствами А., путём перевода их на свою карту. Все предшествующие завладению денежными средствами действия С. были совершены исключительно для достижения указанной цели. О наличии умысла именно на хищение денежных средств свидетельствует тот факт, что С. не просматривал иную информацию, находящуюся в телефоне А., кроме определённых СМС-оповещений.

Ещё одним обстоятельством, указывающим на мошеннический характер действий, является, безусловно, обманный способ совершения преступления, также указывающий на особенности субъективной стороны преступления.

Для преступлений против собственности, совершаемых посредством мобильной связи и сети «Интернет», как и для преступлений в сфере ком-

---

[1] Комментарий к уголовному кодексу Российской Федерации / С. А. Боженок, Ю. В. Грачева, Л. Д. Ермакова и др.; отв. ред. А. И. Рарог. 10-е изд., перераб. и доп. — М.: Проспект, 2015. — С. 725.

[2] Там же.

[3] Приговор Братского городскоого суда Иркутской области от 23.03.2015 по делу № 1-130/2015. [Электронный ресурс]. — Режим доступа: http://sudact.ru (дата обращения 06.03.2017).

пьютерной информации, характерна вина в виде прямого умысла. Косвенный умысел возможен лишь по отношению к последствиям в случаях, когда посягательство на компьютерную информацию осуществляется лишь в целях завладения имуществом. Так, например, возможна ситуация, когда лицо, посягающее на денежные средства потерпевшего, предвидит последствия в виде уничтожения информации, не желает, но сознательно допускает их наступление или относится к ним безразлично. Не исключена вероятность и неосторожного отношения к последствиям, как легкомысленного, так и небрежного. Но, учитывая, что посягательства на компьютерную информацию в целях хищения имущества или причинения имущественного ущерба, осуществляются, как правило, лицами, обладающими определённым уровнем знаний и способными осознавать характер результата своих действий, то преступная небрежность даже по отношению к последствиям маловероятна.

Субъект преступлений против собственности и преступлений в сфере компьютерной информации не обладает какими-либо специфическими признаками.

Разумеется, можно вести речь и о субъекте квалифицированного состава мошенничества в сфере компьютерной информации, предусмотренного ч. 3 ст. 159^6 УК РФ, т. е. о лице, совершающем преступление с использованием своего служебного положения. Указание на подобный субъект присутствует и в статьях о преступлениях в сфере компьютерной информации. Так, ч. 3 ст. 272 УК РФ и ч. 2 ст. 273 УК РФ содержат рассматриваемый квалифицирующий признак. Использование служебного положения при совершении неправомерного доступа к компьютерной информации состоит в том, что виновный получает к ней доступ, незаконно используя права, предоставленные ему исключительно в силу выполняемой им служебной деятельности. Таким лицом, например, может выступать главный бухгалтер коммерческой организации, имеющий доступ к компьютерной информации о счетах организации и право пользования ею в интересах организации, однако использует своё служебное положение для незаконного обогащения за счёт указанной компьютерной информации.

Примером может служить приговор в отношении Р. и Л., совершивших мошенничество в сфере компьютерной информации, т. е. хищение чужого имущества путём ввода, модификации компьютерной информации, группой лиц по предварительному сговору, лицом, с использованием своего служебного положения Р. на основании приказа (распоряжения) о приёме работника на работу занимал должность оператора-кассира и в силу своего служебного положения был наделён полномочиями лица, осуществляющего организационно-распорядительные и административно-хозяйственные функции (обязанности) в коммерческой организации.

Л. на основании приказа (распоряжения) о приёме работника на работу и трудового договора занимал должность управляющего отделом ком-

пании, оказывающей услуги сотовой связи и в силу своего служебного положения был наделён полномочиями лица, осуществляющего организационно-распорядительные и административно-хозяйственные функции (обязанности) в коммерческой организации.

Р. и Л., вступив в предварительный преступный сговор, разработали преступный план, согласно которому, используя своё служебное положение, имея доступ к компьютерной программе, предназначенной для полного цикла обслуживания абонентов оператора сотовой связи, решили искать в ней заблокированные абонентские номера оператора сотовой связи, на лицевых счетах которых находились денежные средства, принадлежащие абонентам, после чего, осознавая, что владелец указанного абонентского номера не сможет воспользоваться денежными средствами, находящимися на данном лицевом счёте, незаконно, без соответствующих заявлений абонентов оператора сотовой связи, намеревались производить на рабочем месте в офисах обслуживания и продаж, с помощью компьютерной программы разблокировку этих абонентских номеров, тем самым модифицируя компьютерную информацию. После этого Р. и Л., преследуя корыстную цель в виде личного материального обогащения, без соответствующих заявлений абонентов оператора сотовой связи, намеревались осуществлять замену сим-карт разблокированных абонентских номеров на новые сим-карты, имевшиеся в их пользовании, путем ввода в компьютерной программе нового серийного IMSI номера сим-карты, получая, таким образом, возможность распоряжаться денежными средствами, находившимися на лицевых счетах разблокированных абонентских номеров оператора сотовой связи, принадлежащих абонентам. При этом Р. и Л. решили с целью совершения хищения денежных средств с абонентских номеров оператора сотовой связи, принадлежащих абонентам, осуществлять доступ к программе также под учётной записью других специалистов. Для обеспечения беспрепятственной и успешной реализации данного пункта плана, Л., должен был приказать подчинённым сотрудникам офиса сообщить ему свои индивидуальные логин и пароль для работы в программах, аргументируя это производственной необходимостью. После замены сим-карт Р. и Л. намеревались осуществлять переводы денежных средств с лицевых счетов разблокированных абонентских номеров на зарегистрированные на них банковские карты и телефонные номера, тем самым совершать хищения денежных средств с использованием своего служебного положения. Похищенные денежные средства Р. и Л. планировали обратить в свою пользу и распорядиться ими по своему усмотрению[1].

[1] Приговор Пролетарского районного суда г. Тулы от 24.03.2016 № 1-32/2016 по делу Р. И Л. [Электронный ресурс]. — Режим доступа: http://sudact.ru/regular/doc/V7owrOu68Cr/ (дата обращения: 11.03.2017).

Говоря о разграничении составов преступлений против собственности, совершаемых посредством мобильной связи и сети «Интернет», и составов преступлений в сфере компьютерной информации, необходимо обратить внимание на отличие составов рассматриваемой группы имущественных преступлений между собой. Так, судами часто допускаются ошибки в квалификации кражи и мошенничества в банковской сфере.

Показателен пример Н., который обратился с просьбой к С. воспользоваться банковской картой последнего с целью установления интернет-обслуживания. При этом Н. дезинформировал С., который, не подозревая о преступных намерениях Н., осуществил в банкомате с использованием своей карты операции, продиктованные Н., и предоставил ему две выданные банкоматом квитанции с данными о своей банковской карте и о находящихся на ней денежных средствах. Завладев конфиденциальной информацией, Н. перевёл денежные средства в размере 12 тыс. руб. с банковской карты С. на банковскую карту своего знакомого З. через Интернет. Далее Н., используя банковскую карту З., получил похищенные денежные средства в банкомате. В результате тайного хищения потерпевшему С. причинён значительный ущерб.

Президиум Алтайского краевого суда переквалифицировал действия Н. с п. «в» ч. 2 ст. 158 УК РФ на ч. 2 ст. 159^6 УК РФ, в обоснование своего решения указав следующее.

Судом действия Н. квалифицированы по ч. 2 ст. 159 УК РФ как хищение чужого имущества, совершённое путём обмана с причинением значительного ущерба потерпевшему. Решение кассационной инстанции о переквалификации действий Н. с ч. 2 ст. 159 УК РФ на ч. 2 ст. 158 УК РФ следует признать ошибочным. Судебная коллегия мотивировала свои выводы тем, что действие осуждённого по изъятию денежных средств является тайным, а обман потерпевшего явился средством облегчения совершения хищения. При этом коллегией не учтён особый способ совершения хищения, выделенный законодателем в отдельный состав преступления и являющийся специальной нормой по отношению к ст. 159 УК РФ.

Как установлено судом, осуждённый путём обмана завладел информацией о реквизитах банковской карты потерпевшего, после чего получил возможность посредством электронной системы через Интернет управлять счётом С. и перевёл с его банковской карты денежные средства на другой счёт. Таким образом, описанный способ хищения свидетельствует о вмешательстве в функционирование средств хранения, обработки, передачи компьютерной информации, что подпадает под действие ст. 159^6 УК РФ[1].

В другом случае суд также переквалифицировал действия обвиняемого со ст. 158 УК РФ на ст. 159^6 УК РФ. Преступление совершено при следующих обстоятельствах. А. увидел ранее ему незнакомого Г., разговаривающего

[1] *Болсуновская Л. М.* Указ. соч. С. 13.

по сотовому телефону, и из корыстных побуждений решил открыто похитить у Г. сотовый телефон. А. подбежал к Г., выхватил у него из руки сотовый телефон и скрылся с места совершения преступления, распорядившись похищенным имуществом по своему усмотрению. В результате умышленных преступных действий А. потерпевшему Г. был причинён имущественный ущерб на общую сумму 2490 руб. После совершения грабежа в отношении Г., А. обнаружил в похищенном сотовом телефоне СМС-сообщения с номера 900 услуги «Мобильный банк» о балансе счёта банковской карты ОАО «Сбербанк России» Г. и по внезапно возникшему корыстному умыслу решил совершить хищение денежных средств со счёта банковской карты ОАО «Сбербанк России» на имя Г. Осуществляя задуманное, А., посредством использования услуги «Мобильный банк», ввёл команду на перевод денежных средств в размере 7000 руб. со счёта банковской карты ОАО «Сбербанк России» на имя Г. на счёт карты ОАО «Сбербанк России», находящейся в его пользовании. После этого, используя банкомат «Сбербанка России», обналичил денежные средства, переведённые со счёта банковой карты Г. в сумме 7 тыс. руб. и присвоил себе, таким образом совершив их хищение. В дальнейшем похищенными денежными средствами А. распорядился по собственному усмотрению.

На судебном заседании государственный обвинитель изменила предъявленное обвинение по обстоятельствам хищения со счёта банковской карты ОАО «Сбербанк России» на имя Г. денежных средств, попросив суд переквалифицировать действия подсудимого А. с п. «в» ч. 2 ст. 158 УК РФ на ч. 2 ст. 159.6 УК РФ.

По факту хищения денежных средств с банковской карты Г. действия подсудимого А. подлежат квалификации по ч. 2 ст. 159.6 УК РФ, т. к. он совершил мошенничество в сфере компьютерной информации, т. е. хищение чужого имущества путём ввода компьютерной информации и иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, с причинением значительного ущерба гражданину[1].

Кроме того, следует отграничивать как преступления в сфере компьютерной информации, так и «компьютерное» мошенничество от неправомерного оборота средств платежей (ст. 187 УК РФ). Постановление Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» предлагает разъяснения по поводу особенностей квалификации подобных деяний. Так, если хищение денежных средств с помощью банковских карт осуществлено путём внедрения

[1] Приговор Железнодорожного районного суда г. Читы (Забайкальский край) № 1-465/2015, 1-64/2016 от 29.04.2016 по делу А. [Электронный ресурс]. — Режим доступа: http://sudact.ru/regular/doc/Sdk2JBd3c3ru/ (дата обращения: 09.12.2016).

в информационную банковскую систему, либо путём создания, использования или распространения вредоносных компьютерных программ, деяние следует квалифицировать в зависимости от обстоятельств дела по ст. 272 или 273 УК РФ при наличии одного из следующих условий: если в результате неправомерного доступа к охраняемой законом компьютерной информации произошло её уничтожение, блокирование, модификация, либо копирование.

Показательно в этом отношении дело в отношении К., рассмотренное Сарапульским городским судом Удмуртской Республики.

К. совершил неправомерный оборот средств платежей, т. е. изготовление в целях использования поддельных платёжных распоряжений о переводе денежных средств, предназначенных для неправомерного осуществления перевода денежных средств при следующих обстоятельствах.

В июле 2015 г. К. принято решение № 1 Единственного участника об учреждении ООО «К». В Межрайонной инспекции Федеральной налоговой службы № 5 по Удмуртской Республике, зарегистрировано юридическое лицо — ООО «К», в соответствии с чем в Единый государственный реестр юридических лиц внесена запись о создании юридического лица за основным государственным регистрационным номером, ООО поставлено на учёт в соответствии с Налоговым кодексом РФ в налоговом органе. К. назначен директором указанной организации. Согласно Уставу ООО «К» директор общества без доверенности действует от имени Общества, в том числе представляет его интересы и совершает сделки; выдаёт доверенности на право представительства от имени Общества, в том числе доверенности с правом передоверия; издаёт приказы о назначении на должности работников Общества, об их переводе и увольнении, применяет меры поощрения и налагает дисциплинарные взыскания; осуществляет иные полномочия, не отнесённые к компетенции общего собрания участников.

Также в июле 2015 г. был открыт расчётный счёт ООО, предоставлены услуги расчётно-кассового обслуживания в валюте РФ дистанционного банковского обслуживания с использованием Системы «Сбербанк Бизнес-онлайн» с предоставлением логина и вариантом защиты системы и подписания документов в виде одноразовых СМС-паролей, поступающих на абонентский номер, принадлежащий директору ООО «К» К.

К., осуществляя полномочия директора, будучи единоличным руководителем ООО «К», дал указание бухгалтеру, не осведомлённой о его преступном умысле, подготовить платёжное поручение о перечислении денежных средств на сумму 635 000 руб. с расчётного счёта ООО «К» на расчётный счёт индивидуального предпринимателя «И», с указанием в качестве назначения платежа: «выдача денежных средств под отчёт» с целью вывода денежных средств из контролируемого оборота и придания своим действиям вида законности, достоверно зная, что И. не является работником ООО «К» и правовых оснований, предусмотренных законом для перевода

денежных средств с расчётного счёта ООО «К» на расчётный счёт ИП «И» у него не имеется, а сама финансовая операция осуществляется с целью обналичивания денежных средств и использования их в дальнейшем по своему усмотрению для получения имущественной выгоды, не связанной с коммерческой деятельностью, подконтрольной организации ООО «К». Бухгалтер, полагая, что действует правомерно, согласно указаниям К. сформировала платёжное поручение, ею был осуществлён перевод денежных средств, что повлекло противоправный вывод денежных средств ООО «К» в неконтролируемый оборот.

Суд признал К. виновным в совершении преступления, предусмотренного ч. 1 ст. 187 УК РФ и приговорил к одному году лишения свободы со штрафом в 100 тыс. руб.[1].

В первую очередь разграничение проводится по признакам объекта, а именно по предмету — средству платежа. Если при мошенничестве в сфере компьютерной информации мы говорим о различного рода манипуляциях с компьютерной информацией, позволяющих преступнику завладеть чужим имуществом, то применительно к ст. 187 УК РФ необходимо учитывать, что подобное завладение осуществляется при помощи неправомерного оборота средств платежей, т. е. поддельных платёжных карт, распоряжений, электронных средств и т. д. При мошенничестве о средстве платежа не идёт речи, достаточно манипуляций с информацией. При неправомерном же обороте средств платежей именно указанные средства будут предметом преступления и одновременно орудием завладения имуществом в рамках другого преступления — кражи или мошенничества. В приведённом выше примере представляется спорной позиция суда о вменении лицу только ст. 187 УК РФ, тогда как в его действиях наряду с неправомерным оборотом средства платежа (платёжного поручения) усматриваются ещё и признаки мошенничества. Несмотря на то, что ст. 187 УК РФ можно назвать своего рода специальной нормой по отношению к ст. 159^6 УК РФ, подобная точка зрения также представляется спорной по ряду моментов. Во-первых, мошенничество в сфере компьютерной информации и неправомерный оборот средств платежей посягают на разные объекты. В первом случае — это отношения собственности, во втором — нормальные отношения в сфере экономической деятельности. Во-вторых, мошенничество — материальный состав преступления, для его завершения необходимо, чтобы виновный завладел имуществом или правом на имущество иного лица. Неправомерный оборот средств платежей — формальный состав. Преступление окончено с момента изготовления, хранения, транспортировки или сбыта поддельного

[1] Приговор Сарапульского городского суда Удмуртской Республики от 07.10.2016 № 1-256/16 по делу К. [Электронный ресурс]. — Режим доступа: http://sudact.ru/regular/doc/p5StY3oz79UV/ (дата обращения: 10.03.2017).

средства платежа, независимо от того, наступили последствия в виде незаконного завладения имуществом или нет.

Согласно упомянутому постановлению Пленума Верховного Суда РФ «О мошенничестве, присвоении и растрате» хищение чужих денежных средств, находящихся на счетах в банках, путём использования похищенной или поддельной кредитной либо расчётной карты следует квалифицировать как мошенничество только в тех случаях, когда лицо путём обмана или злоупотребления доверием ввело в заблуждение уполномоченного работника кредитной, торговой или сервисной организации (например, в случаях, когда, используя банковскую карту для оплаты товаров или услуг в торговом или сервисном центре, лицо ставит подпись в чеке на покупку вместо законного владельца карты либо предъявляет поддельный паспорт на его имя). Изготовление в целях сбыта или сбыт поддельных кредитных или расчётных банковских карт квалифицируется по ст. 187 УК РФ. Изготовление лицом поддельных банковских расчётных либо кредитных карт для использования в целях совершения этим же лицом преступлений, предусмотренных ч. 3 или ч. 4 ст. 159 УК РФ, следует квалифицировать как приготовление к мошенничеству. Если лицо использовало похищенную или поддельную кредитную либо расчётную карту, но по независящим от него обстоятельствам ему не удалось обратить в свою пользу или в пользу других лиц чужие денежные средства, содеянное в зависимости от способа хищения следует квалифицировать как покушение на кражу или мошенничество по ч. 3 ст. 30 УК РФ и соответствующей части статьи 158 или статьи 159 УК РФ. Сбыт поддельных кредитных либо расчётных карт, а также иных платёжных документов, не являющихся ценными бумагами, заведомо непригодных к использованию, образует состав мошенничества и подлежит квалификации по соответствующей части статьи 159 УК РФ. В случае, когда лицо изготовило с целью сбыта поддельные кредитные либо расчётные карты, а также иные платёжные документы, не являющиеся ценными бумагами, заведомо непригодные к использованию, однако по независящим от него обстоятельствам не смогло их сбыть, содеянное должно быть квалифицировано в соответствии с ч. 1 ст. 30 УК РФ как приготовление к мошенничеству, если обстоятельства дела свидетельствуют о том, что эти действия были направлены на совершение преступлений, предусмотренных ч. 3 или ч. 4 ст. 159 УК РФ.

Соответственно в ином случае изготовление, хранение, транспортировку или сбыт поддельных средств платежей следует квалифицировать по совокупности со ст. 159 УК РФ. Если же преступление совершено с использованием компьютерной информации, то квалификация должна осуществляться по совокупности со ст. 159^6 УК РФ.

Подтверждением тому служит приговор Железнодорожного районного суда г. Орла в отношении Б., который, являясь главой крестьянского (фермерского) хозяйства, под видом осуществления производственной и иной хо-

зяйственной деятельности в форме крестьянского (фермерского) хозяйства по разведению крупного рогатого скота, решил совершить хищение бюджетных денежных средств с использованием недостоверных сведений.

Б. предоставил в отдел развития сельских территорий Управления сельского хозяйства Департамента сельского хозяйства Орловской области заявку на участие в конкурсном отборе долгосрочной областной целевой программы «Развитие крестьянских (фермерских) хозяйств и других малых форм хозяйствования в сельской местности в Орловской области на 2012—2015 годы». Кроме того, им был представлен пакет документов, содержащих недостоверные сведения, в частности, бизнес-план инвестиционного проекта. После того, как конкурсная комиссия Департамента одобрила его участие в программе, Б. заключил с Департаментом соглашение о предоставлении ему гранта на создание и развитие крестьянского (фермерского) хозяйства. По указанному соглашению, не имея намерений и возможности осуществлять взятые на себя обязательства, Б. обязался в срок до конца сентября 2013 г. приобрести необходимый инвентарь на средства гранта в размере 922 500 руб. Указанные средства поступили на расчётный счёт Б., который распорядился ими по своему усмотрению, причинив ущерб в крупном размере. Далее Б. обратился в ООО «Промкомплекс» и предложил условия, по которым ООО «Промкомплекс» оформляет с ним договор и сопутствующие документы на куплю-продажу инвентаря, а Б. перечислит денежные средства на расчётный счёт ООО «Промкомплекс», которые за вознаграждение в размере 3 % от суммы, должны быть ему возвращены наличными без фактического исполнения каких-либо обязательств по договору. Согласившись с условиями Б., сотрудник ООО «Промкомплекс» изготовил и подписал от имени директора: договор купли-продажи на сумму 1 028 500 руб.; дополнительное соглашение к указанному договору; транспортную накладную; опись к акту приёма-передачи; счёт-фактуру; товарную накладную; акт приёма-передачи к договору купли-продажи. Вышеуказанные документы были переданы Б. сразу же после изготовления. Затем Б. перечислил на расчётный счёт ООО «Промкомплекс» денежные средства соответственно в суммах 628 500 руб. и 400 000 руб. якобы в счёт оплаты инвентаря по вышеуказанному договору. Однако фактически ООО «Промкомплекс» подсудимому ничего не продавало. С целью возврата данных денежных средств подсудимому, часть их представитель ООО снял наличными в банке по чекам, другую часть перечислил платёжным поручением на расчётный счёт. Действия Б. были квалифицированы судом по ч. 1 ст. 187 УК РФ и по ч. 3 ст. 159^6 УК РФ[1].

[1] Приговор Железнодорожного районного суда г. Орла от 30.05.2016 № 1-20/2016 по делу Б. [Электронный ресурс]. — Режим доступа: http://sudact.ru/regular/doc/66yDzpTT6qJx/ (дата обращения: 11.03.2017).

Иные преступления против собственности, совершаемые с использованием компьютерной информации, следует отграничивать от присвоения и растраты (ст. 160 УК РФ). Так, к примеру, хищение денежных средств возможно сотрудником коммерческой организации, которому были вверены денежные средства. Показателен в этом отношении приговор по делу А., которая, являясь пользователем социальной сети «Одноклассники», имея профиль под никнеймом «Интернет-магазин «Престиж», получила от Б. на систему «QIWI-кошелёк» денежные средства в сумме 4004 руб. с целью приобретения товара. А. перенаправила заказ на сайт интернет-магазина «Престиж», однако данного товара в наличии не оказалось, о чём Б. в известность не поставила. После чего А., зная, что денежные средства в сумме 4004 руб. вверены ей Б. для приобретения товара, присвоила их, переведя со своего «QIWI-кошелька» на свой лицевой счёт, обратив в свою собственность[1].

Следует отграничивать преступления в сфере компьютерной информации, повлёкшие её уничтожение, от умышленного уничтожения или повреждения имущества. В данном случае разграничение проводится по предмету посягательства. Предметом преступлений против собственности, в том числе и мошенничества в сфере компьютерной информации может выступать только имущество как таковое или право на имущество, подтверждённое документально, информация же, тем более компьютерная, предметом таких преступлений не является. Поэтому квалификация действий лица, совершившего неправомерный доступ к компьютерной информации и последующее её уничтожение, не может осуществляться по ст. 167 УК РФ.

Важным моментом также является разграничение различных составов мошенничества между собой. В частности ст. 159 УК РФ следует отграничивать от ст. 159^{6} УК РФ. Особенно это касается случаев обмана потерпевших путём направления им ложных СМС-сообщений (о болезни близкого родственника, о ДТП, о блокировке банковской карты и т. п.). При квалификации подобных деяний возникает проблема не столько практического, сколько теоретического характера. В предыдущем параграфе упоминалось о том, что СМС-сообщение, по сути, представляет собой компьютерную информацию, путём ввода которой преступник достигает желаемого результата — обмана потерпевшего, совершая хищение денежных средств последнего. Вместе с тем, только лишь путём ввода данной информации преступник не может совершить хищение (в отличие от ввода информации, например, в систему «Сбербанк-онлайн»). Для завладения денежными средствами всё же необходимо введение потерпевшего в заблуждение относительно истинных обстоятельств дела, которое может и не произойти. Таким образом, в данном случае набор и отправка СМС-сообщения так же, как простой телефонный звонок с соответствующей информацией при отсут-

[1] *Простосердов М. А.* Указ. соч. С. 85.

ствии последствий можно расценивать лишь как покушение на преступление. В связи с отсутствием необходимых признаков объективной стороны представляется целесообразным подобные факты квалифицировать всё же по ст. 159 УК РФ, т. е. по общей норме.

Подобной позиции придерживается и судебная практика. Так, Трусовским районным судом г. Астрахани Н. и М. были осуждены за совершение мошенничества группой лиц по предварительному сговору по ч. 2 ст. 159 УК РФ.

Так, Н., находясь в ФКУ ИК-№ N. УФСИН России, где отбывал наказание за ранее совершённое преступление, посредством телефонной связи вступил в предварительный преступный сговор с М. на совершение хищения чужого имущества путём обмана. Н. и М. разработали план совершения преступления и распределили между собой роли. Согласно разработанному плану и распределению ролей Н. посредством телефонной связи должен был звонить на случайно выбранные стационарные абонентские номера телефонов и, представившись следователем, сообщать гражданам ложную информацию о совершении якобы их родственником преступления и о необходимости передачи денежных средств следователю за решение вопроса о непривлечении его (родственника) к уголовной ответственности. Далее в случае получения положительного ответа от потенциального потерпевшего, Н. должен был входе телефонных переговоров с потерпевшим договориться о сумме денежных средств, предназначенной якобы для передачи следователю и выяснить адрес места его (потерпевшего) жительства, с целью последующего получения от него (потерпевшего) денежных средств. После чего Н. должен был передавать полученную информацию об обманутом лице и месте его жительства М. М. должна была по указанию Н. прибыть по месту жительства потерпевшего и получить денежные средства, а затем скрыться с места происшествия. После совершения хищения часть похищенных денежных средств М. должна была перевести на счета абонентских телефонных номеров сотовой связи, находящихся в пользовании Н., а оставшуюся часть оставить себе.

Во исполнение задуманного Н. осуществил телефонный звонок на стационарный телефон потерпевшей Ю. и сообщил ложную информацию о том, что он является следователем, что её сына С. задержали за совершённое преступление, и за решение вопроса о невозбуждении в отношении его уголовного дела, ей необходимо передать ему (Н.) денежные средства.

Ю. сообщила Н., что у неё имеются денежные средства в сумме 50 тыс. руб., которые она готова передать, а также адрес своего места жительства. М. встретилась с Ю., от которой получила 50 тыс. руб. и скрылась. Впоследствии часть похищенных денежных средств М. перечислила на ли-

цевой счёт неустановленных абонентских номеров сотовой связи, находящихся в пользовании Н., а оставшуюся часть оставила себе[1].

Приведённые примеры свидетельствуют о необходимости учёта всех признаков состава преступления при отграничении смежных составов друг от друга, а также значения данных признаков в каждом конкретном случае.

Таким образом, основными критериями отграничения посягательств на имущество от преступлений в сфере компьютерной информации выступают:

— объект посягательства (в обоих случаях объектом будет являться нормальный обмен компьютерной информацией, однако при посягательстве на собственность указанный объект будет выступать в качестве дополнительного);

— предмет преступления;

— особенности объективной стороны преступления (при посягательстве на имущество преступление в сфере компьютерной информации возможно рассматривать как часть способа преступления);

— субъективная сторона (при квалификации преступления необходимо установить направленность умысла).

Кроме того, необходимо отграничивать составы преступлений против собственности, совершаемые с использованием сети «Интернет» или посредством мобильной связи, друг от друга, исходя из особенностей способа их совершения.

[1] Приговор Трусовского районного суда г. Астрахани от 27.09.2016 № 1-176/2016 по делу Н. и М. [Электронный ресурс]. — Режим доступа: http://sudact.ru/regular/doc/3eGvCqZG7454/ (дата обращения: 22.03.2017).

ГЛАВА 2. ОТДЕЛЬНЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ ПРОТИВ СОБСТВЕННОСТИ, СОВЕРШАЕМЫХ ПОСРЕДСТВОМ МОБИЛЬНОЙ СВЯЗИ И СЕТИ «ИНТЕРНЕТ»

1. Теоретические вопросы квалификации преступлений против собственности, совершаемых посредством мобильной связи и сети «Интернет»

Квалификации преступления — это установление и юридическое закрепление точного соответствия между признаками совершённого деяния и признаками состава преступления, предусмотренного уголовно-правовой нормой.

Процесс квалификации преступлений должен осуществляться с соблюдением принципов истинности, точности, полноты, субъективного вменения, недопустимости двойного вменения, толкования всех сомнений в пользу лица, совершившего общественно опасное деяние.

Следуя наиболее распространённому алгоритму квалификации, в первую очередь рассмотрим объективную сторону деяния.

Преступления против собственности, совершаемые посредством мобильной связи и сети «Интернет», в первую очередь характеризуются способом.

При оценке способа совершения преступления необходимо выяснить следующие обстоятельства:

— совершено ли преступление с использованием компьютерной информации;

— являлся ли доступ к компьютерной информации, с помощью которого совершено имущественное преступление, правомерным или неправомерным;

— выдвигались ли преступником требования передачи имущества или права на имущество посредством мобильной связи или сети «Интернет»;

— использовал ли преступник при реализации своего умысла угрозы собственнику или иное психическое насилие;

— каковы последствия совершённого деяния;

— существует ли причинная связь между совершённым деянием и наступившими последствиями.

Что касается первой позиции, то из неё вытекает ещё ряд вопросов:

— являлось ли использование компьютерной информации способом совершения преступления;

— способом совершения какого именно преступления являлось использование компьютерной информации;

— являлась ли компьютерная информация средством совершения преступления;

— что являлось орудием совершения преступления и существовало ли оно в принципе;

— являлась ли компьютерная информация предметом совершения преступления.

Последний вопрос относится скорее к объекту преступления, однако, все элементы состава преступления находятся в тесной взаимосвязи и так или иначе пересекаются.

Итак, отвечая на первый вопрос «совершено ли преступление с помощью компьютерной информации?», предположим, что совершено (в ином случае, в рамках нашей работы оно бы нас не интересовало). При ответе на данный вопрос прежде всего нам нужно, опираясь на примечание к ст. 272 УК РФ, вспомнить определение компьютерной информации: «Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

Для того чтобы ответить на первый подвопрос, нам нужно выяснить особенности субъективной стороны, потому как именно направленность умысла в данном случае будет указывать на характер компьютерной информации как признака преступления. Исходя из особенностей субъективной стороны (о которой будет сказано далее), можно сделать один из следующих выводов:

— компьютерная информация является средством совершения преступления, т. е. она важна не сама по себе, а как основа для последующего результата;

— компьютерная информация является предметом посягательства.

Последний вариант указывает нам на то, что содеянное будет являться преступлением в сфере компьютерной информации, первый же вариант предполагает, что преступление носит иной характер, в частности, имущественный.

Ответить на вопросы о компьютерной информации как средстве или предмете преступления нам также поможет изучение субъективной стороны деяния, а именно — направленность умысла.

Орудием преступления в сфере компьютерной информации может быть любое техническое средство (например, USB-носитель, на котором находится программа «вирус», предназначенная для уничтожения такой информации, либо кардридер, предназначенный для несанкционированного копирования информации и её последующего использования, и т. п.). Хотя мнения учёных по данному вопросу расходятся. Так, В. В. Хилюта предлагает считать именно компьютерную информацию саму по себе орудием преступления. «В роли же орудия совершения преступления в сфере компьютерной информации выступают команды, вводимые с клавиатуры или с помощью звуковых сигналов, различного рода «вирусные» и «троянские» про-

граммы, а также иная информация, способная осуществить неправомерное воздействие на предмет преступления против собственности. Специфические особенности орудия совершения преступления заставили многих говорить о своеобразном способе совершения преступлений против собственности с использованием средств компьютерной техники»[1]. Позволим себе не согласиться с данной позиций, проведя аналогию с иными преступлениями, не связанными с компьютерной сферой. Так, вызывает сомнения, что яд, подсыпанный в напиток с целью убийства, будет являться орудием. В данном случае уместно говорить о средстве. Аналогичная ситуация имеет место в случае завладения имуществом, совершённого с применением насилия к потерпевшему. Насилие будет выступать средством совершения преступления, а вот нож, применяемый в процессе этого насилия — орудием. Так же и с компьютерной информацией.

Орудия совершения преступления может и вовсе не быть. Так, например, если преступник с целью получить доступ к счетам потерпевшего использует незаконно полученный логин и пароль, то в данном случае речь идёт только об информации (логине и пароле) как средстве совершения преступления.

Второй вопрос квалификации по объективной стороне посвящён правомерности или неправомерности доступа к компьютерной информации. Этот вопрос тесно переплетается с особенностями субъекта преступления. Необходимо установить, имело ли лицо право доступа к той или иной компьютерной информации, если да, то в каком объёме. Также оценке должен повергнуться и факт использования лицом тех или иных средств и орудий для получения доступа к информации. Поскольку на эти вопросы мы уже ответили ранее, то остаётся лишь сопоставить полученный результат с особенностями субъекта. Ответ на данный вопрос имеет решающее значение для разграничения преступлений против собственности и преступлений в сфере компьютерной информации, а также для установления в действиях лица одного преступления или их совокупности.

Следующий вопрос — о выдвижении требований — должен быть рассмотрен для выявления признаков вымогательства в действиях преступника либо для того, чтобы убедиться в отсутствии таких признаков.

Так, например, неправомерный доступ к компьютерной информации и последующее завладение ею могут быть совершены в целях шантажа потерпевшего. В данном случае наряду с неправомерным доступом к компьютерной информации действия лица должны быть квалифицированы как вымогательство.

Вместе с тем, указанные особенности также нужно выяснять с учётом субъективной стороны преступления, исходя из направленности умысла.

---

[1] *Хилюта В. В.* Хищение с использованием компьютерной техники или компьютерное мошенничество? // Библиотека криминалиста. — 2013. — № 5 (10). — С. 23.

Аналогичным образом и с той же целью решается вопрос об использовании преступником угроз или иных способов психического насилия в отношении потерпевшего. В данном случае важно установить, воспринимались ли угрозы и иное психическое насилие потерпевшим реально.

От деяния перейдём к последствиям. Как преступления против собственности, так и преступления в сфере компьютерной информации являются преимущественно преступлениями с материальным составом. Для первых характерны последствия в виде завладения чужим имуществом, для последних — в виде уничтожения, блокирования, модификации либо копирования информации. Поэтому важно с целью установления в действиях виновного наличия или отсутствия совокупности преступлений выяснить, какие наступили последствия. Сопоставив последствия со способом действия, мы можем предположить, что имело место, например, мошенничество в сфере компьютерной информации в совокупности с неправомерным доступом к компьютерной информации. Вместе с тем, ряд преступлений возможен и без последствий. Так вымогательство считается оконченным с момента выдвижения требований, создание вирусной программы окончено собственно с момента её создания, т. е. наступления последствий в виде уничтожения информации и т. п. не требуется. В таком случае оценка содеянного осуществляется только по самому действию и характеризующим его признакам.

Рассуждая о последствиях, не стоит забывать, что они должны быть следствием именно рассматриваемого нами деяния, а не результатом случайного стечения обстоятельств или совершенно иного действия. Здесь мы начинаем вникать в сущность причинной связи.

Причинная связь должна устанавливаться, исходя из того, могло ли действие неминуемо повлечь наступивший результат, мог ли результат наступить из-за иного действия или обстоятельства, не связанного с рассматриваемым. Могло ли явиться последствие результатом иного последствия и можем ли мы считать его также последствием рассматриваемого деяния. Если два первых вопроса не вызывают недоумения, то последний вносит некоторую путаницу. О чём идёт речь? Абстрагируясь от рассматриваемой нами группы преступлений, приведём пример с ДТП, когда происходит столкновение двух автомобилей на узком мосту, либо на трамвайных путях, наступает в первую очередь повреждение транспортного средства, во вторую очередь, ввиду повреждения, не позволяющего транспортному средству осуществлять дальнейшее движение, происходит блокирование пути на некоторое время, что, таким образом, может привести ещё к ряду неблагоприятных последствий (например, по мосту передвигался автомобиль скорой медицинской помощи с находящимся в тяжёлом состоянии больным, задержка даже на несколько минут могла обернуться для больного смертельным исходом). Иными словами, само по себе деяние вызвало, по сути, одно последствие, которое, в свою очередь, явилось причиной другого. Выстроилась некая причинно-следственная цепочка. В данном случае

необходимо установить, какие последствия находятся в прямой зависимости от совершённого деяния, и, исходя из отношения виновного к совершённому деянию и его последствиям, определить, какие последствия охватывались его умыслом, какие он допускал, а какие не мог и по обстоятельствам дела не должен был предвидеть.

Возможно, наступление нескольких неблагоприятных последствий одновременно, когда все они не образуют цепочку, а находятся в одном ряду. В таком случае необходимо устанавливать причинную связь между деянием и каждым из этих последствий. Так, например, если в результате неправомерного доступа была скопирована информация, совершено хищение денежных средств и была нарушена тайна переписки, то все три последствия подлежат самостоятельной оценке, а содеянное будет образовывать идеальную совокупность преступлений.

Следующим элементом, по которому мы будем производить квалификацию, является субъективная сторона. Значение субъективной стороны при квалификации преступлений, связанных с компьютерной информацией, и при их разграничении трудно переоценить. Возможно, именно с субъективной стороны следовало бы начинать квалификацию в данном случае, но весьма затруднительно говорить об абстрактном, не изучив имеющееся конкретное. Поэтому мы, придерживаясь общепринятой позиции, всё же начали наш процесс с выявления особенностей объективной стороны. Вместе с тем, рассуждая об этих особенностях, мы не раз ссылались на необходимость исследования субъективной стороны.

Относительно субъективной стороны нас будут интересовать следующие вопросы:

— как лицо относилось к содеянному;

— какой вид умысла имел место и какова его направленность;

— какую преступник преследовал цель;

— имел ли место корыстный мотив при совершении преступления.

Что касается первого вопроса, то, исходя из определения вины, можно сделать вывод, что относилось лицо к содеянному виновно или невиновно. Последний случай означает, что лицо не желало наступления последствий, не предвидело и по обстоятельствам дела не могло и не должно было их предвидеть. К примеру, лицо, направляя электронное письмо, с заложенной в нём программой-«вирусом», не знает об этом факте (программа попала в письмо через неправомерный доступ третьих лиц, к примеру). В результате получения письма адресатом программа-«вирус» уничтожает важную информацию. Подобное действие адресанта не образует состава преступления и является невиновным.

Виновное же причинение вреда, исходя из теории о формах вины, может быть умышленным или неосторожным. Однако рассматриваемая нами категория преступлений может совершаться только умышленно. Невозможно неосторожно завладеть чужим имуществом.

Далее возникает второй вопрос — о виде умысла и его направленности. Проанализировав составы преступлений против собственности, совершаемые посредством мобильной связи или сети «Интернет», мы пришли к выводу, что указанные деяния совершаются исключительно с прямым умыслом, причём в большинстве случаев этот умысел является заранее обдуманным.

Решающим, однако, будет вопрос о цели преступника. В зависимости от того преступного результата, которого он желает достичь, может кардинально меняться квалификация содеянного. Так, если преступник преследовал лишь цель копирования компьютерной информации с целью последующего её использования либо уничтожения такой информации с целью причинить ущерб её собственнику, то в данном случае имеет место преступление в сфере компьютерной информации. Если же компьютерная информация выступала лишь средством совершения посягательства на собственность, и основной целью было именно завладение имуществом, то содеянное образует состав имущественного преступления. Выяснение цели важно и для того, чтобы отграничить, например мошенничество в сфере компьютерной информации от неправомерного доступа к компьютерной информации в целях вымогательства.

Так, Чертановский районный суд г. Москвы вынес обвинительный приговор по ч. 1 ст. 163 УК РФ в отношении Р., совершившего вымогательство, т. е. требование передачи чужого имущества под угрозой повреждения чужого имущества. Преступление совершено при следующих обстоятельствах.

Р., используя вредоносную программу, с помощью которой получил неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в почтовом ящике потерпевшего, а именно данные об учётной записи пользователя устройства Apple (Apple ID), дающей возможность распоряжаться полученной информацией, не имея на то разрешения законного собственника — В., тем самым получил возможность дистанционного доступа к мобильному телефону стоимостью 20 тыс. руб., мобильному телефону стоимостью 30 тыс. руб., мобильному телефону стоимостью 25 тыс. руб., планшетному компьютеру стоимостью 27 тыс. руб., планшетному компьютеру стоимостью 23 тыс. руб., планшетному компьютеру стоимостью 28 тыс. руб. и распоряжаться находящейся на данных устройствах информацией, принадлежащей В.

Затем, имея умысел на незаконное обогащение, связанное с завладением денежными средствами В. путём вымогательства под угрозой повреждения принадлежащих последнему указанных выше электронных устройств путём блокировки, Р. осуществил изменение комбинации персонального пароля для входа в учётную запись, предоставляющую возможность дистанционного управления ими, а затем, под видом утери устройств их законным собственником В., заблокировал их работу, в результате чего последний не смог с указанного момента использовать по прямому назначе-

нию вышеуказанные устройства, чем последнему причинён значительный материальный ущерб на общую сумму 78 тыс. руб.

В последующем Р., используя в качестве средства совершения преступления принадлежащий ему мобильный телефон, и продолжая реализацию задуманного, в ходе телефонного разговора с В., предъявил последнему требование передачи ему денежных средств в сумме 100 тыс. руб. под угрозой неснятия блокировки с принадлежащих В. электронных устройств, т. е. их повреждения. При этом Р., заблокировав устройства, тем самым подтвердил угрозу порчи указанного имущества, создав у В. убеждение в её реальности. Впоследствии был задержан сотрудниками полиции.

Органами следствия действия Р. квалифицированы по ч. 1 ст. 272, ч. 1 ст. 163 УК РФ — вымогательство, т. е. требование передачи чужого имущества под угрозой повреждения чужого имущества.

Государственный обвинитель полагал исключить из предъявленного подсудимому обвинения ч. 1 ст. 272 УК РФ, поскольку неправомерный доступ к охраняемой законом компьютерной информации, повлёкший блокирование компьютерной информации, является способом совершения вымогательства, и квалифицировать действия подсудимого по ч. 1 ст. 163 УК РФ как вымогательство, т. е. требование передачи чужого имущества под угрозой повреждения чужого имущества.

Суд, соглашаясь с мнением государственного обвинителя, исключил из обвинения, предъявленного подсудимому Р., ч. 1 ст. 272 УК РФ, поскольку предусмотренный ч. 1 ст. 272 УК РФ состав преступления как неправомерный доступ к охраняемой законом компьютерной информации, повлёкший блокирование компьютерной информации является способом совершения вымогательства, и квалифицирует действия подсудимого по ч. 1 ст. 163 УК РФ как вымогательство, т. е. требование передачи чужого имущества под угрозой повреждения чужого имущества[1].

Таким образом, цель завладения чужим имуществом стала не только отграничительным признаком, но и затмила собою объект. Последнее, по нашему мнению, в корне неверно. В данном случае невозможно исключить из квалификации ст. 272 УК РФ, потому как посягательства осуществлялись на разные объекты. Полагаем, неуместно говорить здесь о неправомерном доступе лишь как о способе вымогательства, когда речь идёт об идеальной совокупности преступлений. Более того, полагаем, квалификацию следовало осуществлять не по ч. 1 ст. 272, а по ч. 2, как деяние, совершённое из корыстной заинтересованности. Ведь изначально у преступника имелся умысел получить доступ к компьютерной информации для последующего вымогательства.

[1] Практика районных судов г. Москвы. [Электронный ресурс] — Режим доступа: http://urist-msk.pro/pp/cher_163_2.html (дата обращения: 17.03.2017).

Следует акцентировать внимание на мотиве совершения преступления, т. к. именно мотив может не помочь нам в квалификации, а, напротив, сбить с толку.

Так, практически все преступления против собственности совершаются с корыстным мотивом. Преступник преследует цель незаконного обогащения. Вместе с тем ст.ст. 272 и 273 УК РФ также предусматривают такой квалифицирующий признак, как корыстная заинтересованность. В предыдущей главе, рассматривая вопросы разграничения смежных составов, мы говорили о том, что в подобном случае компьютерная информация не выступает средством обмана или злоупотребления доверием, или средством, облегчающим доступ к денежным средствам или иному имуществу, а расценивается как предмет преступления. Потому и корыстную заинтересованность в преступлениях в сфере компьютерной информации следует рассматривать исключительно в соотношении с предметом преступления. В связи с этим, следующим этапом в нашей схеме квалификации является установление объекта посягательства.

Квалифицируя содеянное по признакам объекта, мы должны ответить на следующие вопросы:

— на какие общественные отношения осуществляется посягательство;

— по поводу чего оно осуществляется, т. е. каков предмет преступления;

— имеет ли место дополнительный объект преступления;

— имеет ли место факультативный объект преступления.

Признаком объекта, играющим решающую роль в его установлении, выступит предмет посягательства. Именно по предмету производится отграничение посягательств на собственность от преступлений в сфере компьютерной информации.

Предметом преступлений в нашем случае может выступить имущество, право на имущество либо компьютерная информация. В предыдущей главе мы ответили на вопрос, может ли компьютерная информация рассматриваться как имущество, и пришли к выводу, что, исходя из определения имущества, информация к таковому относиться не может. Поэтому отграничение преступлений по предмету в данном случае не составит труда.

Сложности могут возникнуть, когда сама по себе информация может одновременно выступать предметом разных преступлений. Например, компьютерная информация как таковая, к которой ограничен доступ посторонних лиц, и эта же информация, как источник сведений о частной жизни конкретного лица, которые не могут быть разглашены. В данном случае, полагаем, нужно учитывать особенности объективной стороны деяния, а именно последствия, предусмотренные диспозицией ст. 272 УК РФ, т. е. копирование, блокирование, модификация или уничтожение информации, в ином случае мы можем говорить о неправомерном доступе только как о способе совершения деяния, предусмотренного ст. 137 УК РФ. Однако рассматрива-

емой темы данный вопрос касается посредственно, поэтому не будем на нём останавливаться.

Право на имущество, даже полученное при помощи компьютерной информации, всё же остаётся предметом преступления против собственности, и, независимо от того, реализуется это право, или нет, содеянное не перестаёт считаться преступлением.

Таким образом, исходя из предмета, объектом рассматриваемой группы преступлений должны выступать отношения собственности, или, как мы определяли в предыдущей главе, нормальные отношения по поводу распределения и перераспределения материальных благ.

Отвечая на поставленный нами вопрос о наличии либо отсутствии в содеянном дополнительного объекта, необходимо обратиться к объективной стороне каждого состава преступления из числа входящих в рассматриваемую нами группу. Так, не во всех составах преступлений против собственности, совершаемых посредством сети «Интернет» или мобильной связи, возможно наличие дополнительного объекта. На сегодняшний день только состав вымогательства предусматривает два альтернативных дополнительных объекта:

— жизнь или здоровье человека;

— свобода, честь и достоинство личности.

Но и эти два объекта могут отсутствовать в третьем случае, предусмотренном диспозицией статьи — при угрозе уничтожением или повреждением чужого имущества. Так, в приведённом выше примере о вымогательстве, совершённом путём угрозы не разблокировать электронные устройства потерпевшего, преступник использовал именно последний способ, т. к. блокировку, которую невозможно снять, на наш взгляд, следует относить именно к повреждению имущества.

Известны практике и случаи вымогательства, совершённого с использованием компьютерной информации, доступ к которой получен неправомерным путём, сопряжённого с нарушением тайны переписки. Так, Дзержинский районный суд г. Новосибирска вынес обвинительный приговор в отношении С. по ч. 1 ст. 272 УК РФ, ч. 1 ст. 138 УК РФ и ч. 1 ст. 163 УК РФ.

У С. возник преступный умысел на неправомерный (несанкционированный правообладателем) доступ к охраняемой законом, а именно ст. 23 Конституции РФ, ст. 17 Федерального закона от 27.06.06 № 149 «Об информации, информационных технологиях и о защите информации», п. 1 Указа Президента РФ от 06.03.97 № 188 «Перечня сведений конфиденциального характера компьютерной информации», информации о фактах, событиях и обстоятельствах частной жизни, принадлежащей Л., расположенной в электронной почте, на странице Л. в социальных сетях. С. с целью незаконного получения пароля доступа, зашёл на ящик электронной почты, где обратился к ссылке «Забыли пароль», после чего, действуя по указаниям провайдера социальных сетей интернет-ресурса, с целью восстановления

пароля, выбрал ссылку «Ответ на секретный вопрос», после чего ему было предложено ответить на вопрос «На какой улице родилась?», ответ на который С. был известен из общения с Л., после ответа на поставленный вопрос С. был выслан новый пароль для входа на ящик электронной почты, после чего С. получил возможность незаконного доступа к информации, хранящейся в указанном электронном ящике электронной почты и доступа на интернет-страницу Л. Затем С. заменил пароль доступа к электронному ящику электронной почты и доступ пароля к электронному адресу, тем самым модифицировал информацию, заблокировав доступ законного обладателя Л. к охраняемой законом компьютерной информации об обстоятельствах частной жизни, расположенной в ящике электронной почты интернет-ресурса, принадлежащий Л. и на странице Л. социальной сети, лишив Л. возможности пользоваться ими, после чего С. скопировал с интернет-страницы социальной сети Л. переписку Л. с П. и переместил файл с перепиской к себе на ноутбук. Затем С., располагая сведениями об интимных отношениях между П. и Л., полученных им в результате взлома пароля доступа на интернет-страницу Л., позвонил последнему по телефону и незаконно потребовал от П. передачи ему денежных средств в сумме 80 тыс. руб., при этом в случае отказа высказал угрозу предоставить супруге П. электронную переписку с Л. Далее С. неоднократно осуществлял телефонные звонки со своего телефона на телефон П., продолжая вымогать деньги у последнего, в подтверждение переслал по электронной почте компрометирующую переписку, а также неоднократно отправлял СМС-сообщения на телефон П., в которых выражались незаконные требования о передаче денежных средств за нераспространение сведений.

С. назначил П. встречу, в ходе которой получил от П. 10 тыс. руб., после чего был задержан сотрудниками полиции[1].

В данном случае наряду с несколькими объектами, несколькими предметами посягательства, несколькими действиями, но объединёнными единой целью, в деле фигурируют и двое потерпевших. Каждому из них причинён разный вред, вместе с тем одно преступление явилось предикатным (предшествующим и обусловливающим) по отношению к другому.

Говоря о дополнительном объекте, не следует забывать о том, что важно отличать безопасность компьютерной информации как дополнительного объекта преступления, предусмотренного ст. 159[6] УК РФ от основного объекта преступления, предусмотренного ст.ст. 272—274 УК РФ именно в целях правильной квалификации (установления наличия или отсутствия совокупности преступлений в действиях преступника).

[1] Приговор Дзержинского районного суда г. Новосибирска от 21.12.2012 № 1-705/12 по делу С. [Электронный ресурс] — Режим доступа: https://rospravosudie.com/court-dzerzhinskij-rajonnyj-sud-g-novosibirska-novosibirskaya-oblast-s/act-425470944/ (дата обращения: 18.03.2017).

Что касается факультативного объекта, то он может быть абсолютно любым. Необходимо лишь, внимательно изучив объективную сторону, не упустить деталей. Так, мы уже приводили пример, когда совершается мошенничество в сфере компьютерной информации, но в ходе совершения преступления преступнику стали известны сведения, касающиеся частной жизни потерпевшего, которыми он воспользовался, то в данном случае наряду с нормальным обменом информацией и отношениями собственности будет иметь место и такой объект, как конституционное право человека и гражданина. Но необходимо помнить о том, что указанный объект возможно считать факультативным по отношению к ст. 159^6 УК РФ и основным — по отношению к ст. 138 УК РФ.

Применительно к ч. 3 ст. 159^6 УК РФ в случае использования служебного положения должностным лицом, факультативным объектом выступят интересы государственной службы и службы в органах местного самоуправления.

Примером такого преступления может служить дело Д., занимавшего должность судебного пристава-исполнителя и покушавшегося на совершение мошенничества в сфере компьютерной информации.

Указанное преступление им было совершено при следующих обстоятельствах. Д. работал в должности судебного пристава-исполнителя отдела судебных приставов УФССП России. В силу занимаемой должности владел навыками ведения, обработки и редактирования исполнительного производства в Автоматизированной информационной системе (далее — АИС) программного комплекса отдела судебных приставов, обладал сведениями о служебных реквизитах пароля к учётной записи с расширенными административными правами в АИС.

Д. попросил И., с которым находился в дружеских отношениях, оформить в отделении банка личный расчётный счёт и зарегистрировать в компании мобильного оператора абонентский номер, который попросил подключить к услуге «Мобильный банк» по вышеуказанному расчётному счёту якобы с целью последующего перечисления на данный счёт для Д. денежных средств от третьих лиц по долговым обязательствам. Чтобы скрыть эти намерения, Д. сказал И., что у него имеются кредитные задолженности в банке, в связи с чем он не может на своё имя открыть расчётный счёт. И., не зная о преступных намерениях Д., сам имея кредитные задолженности перед банком и не имея из-за этого возможности на своё имя открыть расчётный счёт, решил помочь Д., пообещав ему подыскать такого человека среди своих знакомых. После этого И., действуя в интересах Д., познакомился с З., которого попросил оформить в отделении банка личный расчетный счет, а также зарегистрировать в компании мобильного оператора абонентский номер, подключить его к услуге «Мобильный банк» по вышеуказанному расчётному счёту, а сим-карту с данным абонентским номером передать И., чтобы он в последующем мог получить денежные средства по своим долговым обязательствам. З. согласился на это предложение.

После этого З. открыл на своё имя расчётный счёт, к которому подключил услугу «Мобильный банк». Реквизиты данного счета З. также передал И., а И. передал Д. реквизиты этого счёта и указанную выше сим-карту.

Д. дождался конца рабочего дня и ухода всех сотрудников из отделения УФССП. Затем, неправомерно используя служебные реквизиты (пароль к учётной записи с расширенными административными правами), незаконно осуществил доступ к АИС ПК ОСП УФССП России, где внёс изменения в постановления о распределении денежных средств, поступающих во временное распоряжение на депозитный счёт УФССП России в части наименования взыскателей по исполнительным производствам, находящимся в отделах ФССП, указав о необходимости перечисления на расчётный счёт, открытый на имя З. взыскиваемых сумм.

Однако преступные действия Д. не были доведены до конца по независящем от него обстоятельствам, т. к. на следующий день сотрудниками УФССП России были обнаружены вышеуказанные изменения, и действия по перечислению денежных средств с депозитного счета УФССП России на личный счёт З. были приостановлены[1].

Несомненно, в данном случае наряду с нормальными имущественными отношениями и безопасностью компьютерной информации, вред причинён также и государственной власти, её авторитету и установленному порядку.

Затронув вопрос о лице, использующем своё служебное положение, считаем необходимым перейти к рассмотрению субъекта преступления.

Особых требований диспозиции статей, предусматривающих ответственность за преступления против собственности, совершаемые посредством мобильной связи и сети «Интернет», не предъявляют. Вместе с тем, как мы выяснили в первой главе, ответственность наступает не всегда одинаковая. Так, мы определили, что к рассматриваемой нами группе преступлений относятся некоторые виды мошенничества, присвоение и растрата, вымогательство, причинение имущественного ущерба путём обмана или злоупотребления доверием. В соответствии со ст. 20 УК РФ возраст уголовной ответственности за указанные деяния установлен с 16 лет, за исключением вымогательства, за совершение которого лицо может быть привлечено к уголовной ответственности с 14-ти лет. Иными особенностями общий субъект данных преступлений не обладает.

Квалифицируя содеянное по признакам субъекта, необходимо обратить внимание на следующие моменты:

— является ли лицо, выполнившее объективную сторону преступления, вменяемым;

— достигло ли указанное лицо возраста уголовной ответственности;

---

[1] Приговор Кировского районного суда г. Астрахани от 08.09.2015 № 1-409/2015 по делу Д. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/ZE0dnyLDpJQQ/ (дата обращения: 19.03.2017).

— обладает ли лицо признаками специального субъекта;

— обладает ли лицо иммунитетом.

О признаках вменяемости свидетельствует справка из соответствующего медицинского учреждения, подтверждающая, что лицо не состоит на учёте ввиду психических заболеваний. При возникновении сомнений во вменяемости лица может быть назначена судебно-психиатрическая экспертиза.

Возраст уголовной ответственности определяется в соответствии со ст. 20 УК РФ. Возраст устанавливается по документам, удостоверяющим личность. При этом необходимо помнить, что лицо считается достигшим определённого возраста с 00 ч 00 мин. дня, следующего за днём рождения лица.

Однако следует помнить также о том, что лицо, достигшее возраста уголовной ответственности, может быть вменяемым, но при этом отставать в психическом развитии. Указанное обстоятельство также может быть установлено в результате судебно-психиатрической экспертизы. Если отставание в психическом развитии будет подтверждено, то, в соответствии с ч. 3 ст. 20 УК РФ, лицо не будет подлежать уголовной ответственности.

Что касается признаков специального субъекта, то их установление необходимо для выявления в действиях лица квалифицирующих или привилегирующих признаков, что, в свою очередь, повлечёт более строгую или более мягкую ответственность.

Рассмотрим признаки специального субъекта, предусмотренные в статьях о преступлениях интересующей нас категории.

Итак, ч. 3 ст. 159^1 УК РФ, ч. 3 ст. 159^3 УК РФ, ч. 3 ст. 159^6 УК РФ, ч. 3 ст. 160 УК РФ предусматривают единственно возможный специальный субъект — лицо, использующее своё служебное положение. Особенности данного признака были рассмотрены нами в предыдущей главе, поэтому останавливаться на них мы не будем.

Необходимо отметить также, что диспозиция ст. 160 также предусматривает специальный субъект — лицо, которому имущество вверено.

Требований к тому, чтобы лицо не имело доступа к той или иной компьютерной информации, в данном случае нет. Напротив, как продемонстрировано в приведённых ранее примерах, виновный по праву может распоряжаться компьютерной информацией, к которой он имеет доступ, вот только использует данную информацию в преступных целях. Так, бухгалтер организации, владеющий информацией обо всех счетах фирмы и всех операциях, проводимых по данным счетам, а также электронной подписью, может выступить субъектом указанного преступления.

Для того чтобы провести квалификацию по признакам специального субъекта, необходимо ответить на следующие вопросы:

— занимает ли лицо государственную должность Российской Федерации, субъекта Российской Федерации;

— обладает ли лицо признаками должностного лица;

— обладает ли лицо статусом государственного или муниципального служащего, не являющегося должностным лицом;

— выполняет ли лицо функции единоличного исполнительного органа, члена совета директоров или иного коллегиального исполнительного органа;

— выполняет ли лицо постоянно, временно либо по специальному полномочию организационно-распорядительные или административно-хозяйственные функции в организациях, указанных в предыдущем пункте;

— связано ли деяние с недобросовестным исполнением лицом своих служебных обязанностей;

— было ли имущество вверено виновному.

Для того чтобы провести квалификацию по признакам специального субъекта, вовсе не обязательны положительные ответы на все поставленные вопросы. Более того, отдельные положения могут быть взаимоисключающими. Так, очевидно, что лицо, являющееся должностным, не может быть одновременно муниципальным служащим, не являющимся должностным лицом. Обязательно следует выяснить, связано ли преступное деяние, совершённое лицом, с выполнением им служебных обязанностей.

Наряду с использованием служебного положения, рассматриваемые статьи обладают ещё рядом квалифицирующих признаков. В связи с этим необходимо уделить внимание квалификации преступлений по квалифицирующим признакам.

Итак, первый признак, присущий всем рассматриваемым нами составам — совершение преступления группой лиц по предварительному сговору.

При квалификации по данному признаку необходимо ответить на следующие вопросы:

— сколько человек принимало участие в совершении преступления;

— все ли участники группы удовлетворяют признакам субъекта преступления (вменяемы ли данные лица, достигли ли возраста уголовной ответственности, обладают ли специальными признаками, необходимыми для признания деяния преступлением);

— имелся ли сговор между участниками группы;

— имело ли место распределение ролей между участниками группы;

— какие действия выполнял каждый участник группы.

Первый вопрос возможно было бы поставить и иначе: принимало ли в преступлении участие одно лицо или более, поскольку группу лиц могут образовывать и двое.

Огромное значение имеет ответ на второй вопрос, поскольку выясненные по нему обстоятельства в зависимости от их сочетания могут кардинальным образом изменить квалификацию. Так, если один из участников группы не достиг возраста уголовной ответственности, при условии, что группа состояла из двух человек, то указанное обстоятельство исключает возможность квалификации по данному признаку. Если для совершения

преступления, например, растраты, необходим специальный субъект (в нашем случае — лицо, которому вверено имущество), а участие в совершении преступления принимало(-и) и иное(-ые) лицо(-а), то признак группы лиц также будет отсутствовать, а действия лиц, не являющихся субъектом растраты, необходимо будет квалифицировать как кражу, а возможно, как мошенничество в сфере компьютерной информации (применительно к нашей ситуации).

Важное значение имеет также и установление наличия предварительного сговора между участниками группы, поскольку в случае отсутствия последнего отсутствует и квалифицированный состав преступления, соответственно, преступники будут подвержены менее строгому наказанию.

Вопросы относительно ролей участников и конкретных действий, выполняемых ими, необходимо выяснить для того, чтобы дифференцировать ответственность каждого из них.

Следующий признак, схожий с рассмотренным выше и присущий всем интересующим нас составам преступлений, — совершение преступления организованной группой.

В указанном случае могут возникнуть следующие вопросы:

- объединены ли действия участников группы единым умыслом и целью;

— обладает ли группа признаком устойчивости;

— все ли лица, являющиеся участниками группы, обладают признаками субъекта преступления;

— какова роль каждого из участников организованной группы.

Большинству из перечисленных вопросов мы уделили внимание ранее.

О признаке устойчивости могут свидетельствовать совершение ею преступлений ранее, распределение ролей между участниками группы, техническая оснащённость.

Рассмотрим пример совершения мошенничества в сфере компьютерной информации организованной группой.

Так, братья Николай и Андрей П., а также гр-н Л. и другие соучастники объединились в устойчивую организованную группу с целью совершения хищений денежных средств, находящихся на счетах юридических и физических лиц, обслуживаемых по электронной платёжной системе «Клиент-банк» через сеть «Интернет», путём несанкционированного ввода, удаления, блокирования, модификации компьютерной информации. При этом в организованной группе имело место чёткое распределение ролей между её участниками. Роль Николая П. как организатора и непосредственного исполнителя преступлений выразилась: в вовлечении в преступную группу лиц, имеющих профессиональные навыки осуществления мошенничества в сфере компьютерной информации; в аренде офисного помещения и размещении в нём средств вычислительной техники и мобильной связи, необходимых для осуществления мошенничества в сфере компьютерной

информации; в приобретении платёжных банковских карт и банковских счетов, заведомо оформленных на подставных лиц, а также электронных ключей системы дистанционного банковского обслуживания к ним; в отслеживании поступления денежных средств на счета подставных лиц и организации их обналичивания в банкоматах; в распределении похищенных денежных средств между членами организованной группы, а также координации деятельности участников организованной группы.

Роль одного из соучастников как исполнителя преступлений выразилась в том, что он, будучи администратором неустановленного сайта, размещённого в информационно-телекоммуникационнойсети «Интернет», содержащего вредоносные программы, должен был обеспечить Николаю П. и второму соучастнику техническую возможность посещения данного ресурса и использования размещённых там вредоносных компьютерных программ в преступных целях.

Роль второго соучастника как исполнителя преступлений выразилась в том, что он должен был, используя вредоносные компьютерные программы, осуществлять скрытое наблюдение и выслеживание пользователей ЭВМ с системой дистанционного банковского обслуживания расчётного счета «Клиент-банк», а также анализировать финансовое состояние и наличие денежных средств на их счетах, после чего, на основании полученных сведений, выбрав конкретную организацию или индивидуального предпринимателя, произвести неправомерный доступ в используемую ими платёжную программу, где от имени владельца тайно сформировать фиктивное электронное поручение на перевод денежных средств на счёт подставных лиц и в случае перевода денег сообщать об этом Николаю П. для организации их обналичивания.

Роль Андрея П. как исполнителя преступлений заключалась в том, что он, получив от Николая П. информацию о факте состоявшегося хищения денежных средств, должен был либо сам обналичивать похищенные денежные средства через банкоматы, либо обналичивать их с помощью Л. под своим непосредственным контролем, используя для этого заранее полученные у Николая П. платёжные банковские карты.

Роль Л. заключалась в обналичивании под контролем Андрея П. похищенных денежных средств через банкоматы.

Конкретная преступная деятельность подсудимых выразилась в следующем.

Николай П. незаконно приобрёл банковские карты ОАО «Сбербанк России» платёжной системы «Сбербанк-Маэстро «Моментум», а также идентификаторы и постоянные пароли к ним, произведя их предварительную авторизацию в системе удалённого доступа типа «Сбербанк-онлайн», позволяющую дистанционно осуществлять расчётные операции с денежными средствами, находящимися на указанных карточных счетах, после чего, передал данные платёжные карты Андрею П., а реквизиты лицевых счетов сообщил иному соучастнику. В свою очередь, этот соучастник, получив

от Николая П. реквизиты счёта, с помощью компьютерного оборудования, используя вредоносные компьютерные программы, заведомо предназначенные для скрытой несанкционированной модификации компьютерной информации, а также нейтрализации средств её защиты, путём дистанционного подключения через информационно-телекоммуникационную сеть «Интернет» осуществил неправомерный доступ к электронной системе управления расчётным счётом «Клиент-банк» ООО РИА «Семейная студия», установленной на ЭВМ, путём ввода заведомо ложных и несоответствующих действительности сведений сформировал в системе управления расчётным счётом «Клиент-банк» данной организации подложное электронное платёжное поручение, внеся в него реквизиты лицевого счета, сведения о назначении платежа и сумму, подлежащую перечислению, после чего незаконно направил данное электронное платёжное поручение для исполнения в Нижегородский филиал Банка «Возрождение» (ОАО). В результате указанных действий с расчётного счета ООО РИА «Семейная студия» в Нижегородском филиале Б. «Возрождение» (ОАО) электронным платёжным поручением на счёт ФИО1, открытого в ОАО «Сбербанк России», в безналичной форме были незаконно переведены денежные средства в общей сумме 267 тыс. 589 руб. 90 коп., которые с указанного времени поступили в распоряжение виновных. После этого Николай П., получив от соучастника информацию о факте поступления безналичного перевода на счёт ФИО1, используя находящиеся у него в распоряжении идентификатор и постоянный пароль, дистанционно перевёл с лицевого счёта ФИО1 часть денежных средств на лицевой счёт ФИО31, после чего позвонил на мобильный телефон Андрея П. и сообщил ему указанную информацию. Получив данную информацию, Андрей П., используя банковские карты ФИО1 и ФИО31, произвёл обналичивание похищенных денежных средств в сумме 267 тыс. 589 руб. 90 коп. через банкомат Московского банка ОАО «Сбербанк России». Таким образом, в результате вышеуказанных мошеннических действий в сфере компьютерной информации у ООО РИА «Семейная студия» были похищены денежные средства на общую сумму 267 тыс. 589 руб. 90 коп.

Подобным образом организованной группой было совершено шесть эпизодов мошенничества в сфере компьютерной информации[1].

При отграничении преступления, совершённого группой лиц по предварительному сговору, от преступления, совершённого организованной группой, установление признаков организованной группы играет решающую роль, поэтому им необходимо уделять особое внимание.

Следует обратить внимание также на такой квалифицирующий признак, как крупный и особо крупный размер. Квалификация по данному при-

[1] Приговор Люблинского районного суда г. Москвы от 07.04.2014 № 1-1/2014. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/IgF7Z3v8VIgZ/ (дата обращения: 09.03.2017).

знаку не должна вызвать затруднений, поскольку в данном случае необходимо ответить лишь на один вопрос — о сумме причинённого ущерба. Крупный и особо крупный размер для целей ст.ст. 159^1, 159^3, 159^6 УК РФ указаны в примечании к ст. 159^1 УК РФ, в соответствии с которым крупным размером признаётся стоимость имущества, превышающая 1 млн 500 тыс. руб., а особо крупным — 6 млн руб. Что касается присвоения или растраты, то крупным размером в данном случае в соответствии с примечанием к ст. 158 УК РФ признаётся стоимость имущества, превышающая 250 тыс. руб., а особо крупным — 1 млн. руб.

Подводя итоги параграфа, необходимо обобщить выводы, к которым мы пришли.

Во-первых, квалификацию преступлений против собственности, совершаемых посредством сети «Интернет» или мобильной связи, уместнее начинать с признаков объективной стороны, следующим этапом должна быть квалификация по признакам субъективной стороны, затем — по признакам объекта и, наконец, по признакам субъекта преступления. В завершении необходимо установить наличие или отсутствие в действиях виновного квалифицирующих или особо квалифицирующих признаков.

Вместе с тем, наряду с первоначальной квалификацией по предложенному нами алгоритму, при окончательной квалификации всё же необходимо ориентироваться на заключения всех необходимых экспертиз, а также заключения специалистов в области компьютерных технологий.

2. Судебная практика по делам о преступлениях против собственности, совершаемых посредством мобильной связи и сети «Интернет»

Поскольку преступления, совершаемые с использованием компьютерной информации, относительно новы для уголовного законодательства России, судебная практика на данном направлении характеризуется отсутствием единообразного подхода к квалификации, во всяком случае такой подход находится лишь на стадии формирования. Вместе с тем стремительная распространяемость преступлений против собственности, совершаемых в информационном пространстве, способствует формированию тенденций к выработке единого понимания правил их квалификации.

Рассмотрим ряд примеров судебной практики, демонстрирующих различные подходы судов к квалификации деяний рассматриваемой категории.

В ряде случаев судами допускаются ошибки в отграничении составов преступлений против собственности друг от друга.

Так, суд квалифицировал по ст. 159 УК РФ действия Н., который находясь в торгово-развлекательном центре, реализуя свой преступный умысел, направленный на хищение денежных средств, обратился с просьбой к С. воспользоваться его банковской картой с целью установления интернет-обслуживания. При этом Н. дезинформировал С., который, не подозревая о преступных намерениях Н., осуществил в банкомате с использованием своей карты операции, продиктованные Н., и предоставил ему две выданные банкоматом квитанции с данными о своей банковской карте и о находящихся на ней денежных средствах. Завладев конфиденциальной информацией, Н. перевёл денежные средства в размере 12 тыс. руб. с банковской карты С. на банковскую карту своего знакомого З. через Интернет. Далее Н., используя банковскую карту З., получил похищенные денежные средства в банкомате. В результате тайного хищения потерпевшему С. причинён значительный ущерб.

Суд кассационной инстанции приговор изменил, усмотрев в действиях Н. признаки кражи, что, на наш взгляд, представляется абсолютно нелогичным ввиду конкретного чётко выраженного способа совершения преступления. Судебная коллегия мотивировала свои выводы тем, что действие осуждённого по изъятию денежных средств является тайным, а обман потерпевшего явился средством облегчения совершения хищения.

Президиум Алтайского краевого суда переквалифицировал действия Н. с п. «в» ч. 2 ст. 158 УК РФ на ч. 2 ст. 159^6 УК РФ по следующим основаниям.

Судебной коллегией не учтён особый способ совершения хищения, выделенный законодателем в отдельный состав преступления и являющийся специальной нормой по отношению к ст. 159 УК РФ.

Осуждённый путём обмана завладел информацией о реквизитах банковской карты потерпевшего, после чего получил возможность посредством электронной системы через Интернет управлять счётом С. и перевёл с его банковской карты денежные средства на другой счёт. Таким образом, описанный способ хищения свидетельствует о вмешательстве в функционирование средств хранения, обработки, передачи компьютерной информации, что подпадает под действие ст. 159^6 УК РФ[1].

Решение Президиума справедливо, поскольку имел место обманный способ завладения имуществом. Обман послужил для облегчения неправомерного доступа к компьютерной информации заведомо с корыстной целью.

Подобная ситуация имеет место и в случае с М., который обвинялся в том, что, используя приложение ICQ (централизованная служба для мгновенного обмена сообщениями в сети «Интернет»), установленное на своём мобильном телефоне, знакомился и устанавливал доверительные отношения

[1] Постановление Президиума Алтайского краевого суда от 03.09.2013 по делу № 44у224/13 // СПС «КонсультантПлюс».

с пользователями ICQ с целью хищения чужого имущества путём обмана. В дальнейшем М. под различными предлогами получал от пользователей ICQ доступ к их учётным записям в данном мобильном приложении, после чего рассылал от имени этих лиц другим пользователям ICQ сообщения в виде просьб о перечислении денежных средств на телефонные номера оператора сотовой связи «Билайн». После поступления денежных средств на подконтрольные М. абонентские номера он распоряжался ими по своему усмотрению. Действия М. справедливо квалифицированы судом как мошенничество в сфере компьютерной информации с причинением значительного ущерба гражданину, совершённое путём обмана и злоупотребления доверием, т. е. как преступление, предусмотренное ч. 2 ст. 159^6 УК РФ[1].

Московским городским судом допущена ошибка в квалификации содеянного Х. как кражи. Преступление совершено при следующих обстоятельствах.

Х. приискал для совершения преступления необходимые комплектующие и материалы, из которых изготовил два приспособления. Первое устройство позволяло получать (перехватывать) информацию, вводимую держателями карт посредством клавиатуры банкомата, а именно ПИН-коды банковских карт, а второе обеспечивало получение (перехват) информации с магнитных полос банковских пластиковых карт.

Затем Х. в дополнительном офисе ОАО АКБ «ХХХ» под видом монтажа устройства, контролирующего доступ в помещение с банкоматом, установил на входную дверь изготовленное им приспособление для получения (перехвата) информации с магнитных полос банковских пластиковых карт. Таким образом, Х. умышленно создал условия, при которых доступ к банкомату дополнительного офиса ОАО АКБ «ХХХ» стал возможен лишь после копирования компьютерной информации с магнитной полосы банковской пластиковой карты в память указанного устройства. Второе изготовленное им приспособление Х. установил непосредственно над экраном лицевой панели банкомата для получения (перехвата) информации, вводимой клиентами банка с клавиатуры банкомата, а именно ПИН-кодов банковских карт, после чего с места преступления скрылся.

Для прохода к банкомату в вышеуказанном офисе клиенты ОАО АКБ «ХХХ» сканировали свои банковские карты через установленное на входной двери Х. приспособление, в результате чего записанная на магнитной полосе пластиковых карт компьютерная информация копировалась в память устройства. Остаток денежных средств на счетах, к которым были прикреплены сканированные карты, варьировался от нескольких рублей до нескольких сотен тысяч рублей и составил в общей сумме 487 тыс. 521 руб. 10 коп.

[1] Приговор суда г. Дагестанские Огни Республики Дагестан от 08.02.2013 № 1-28/2013 по делу М. [Электронный ресурс] — Режим доступа: http://www.gcourts.ru/case/22900134 (дата обращения: 01.03.2017).

При попытке демонтировать установленные им устройства для того, чтобы использовать скопированную и сохранённую в их памяти компьютерную информацию с магнитных полос банковских карт и ПИН-коды к ним с целью тайного хищения в крупном размере находящихся на счетах денежных средств, принадлежащих ОАО АКБ «ХХХ», Х. был задержан и потому довести свой преступный умысел до конца не смог по независящим от него обстоятельствам.

Действия Х. квалифицированы как приготовление к краже в крупном размере, а также за неправомерный доступ к охраняемой законом компьютерной информации, повлёкший копирование компьютерной информации, совершённый из корыстной заинтересованности (ч. 1 ст. 30 УК РФ, п. «в» ч. 3 ст. 158 УК РФ, ч. 2 ст. 272 УК РФ)[1].

Обоснованность подобной квалификации вызывает сомнения именно ввиду обманного способа преступления, поскольку устройства были установлены виновным путём обмана сотрудников организации. Кроме того, через указанные устройства виновный неправомерно получал компьютерную информацию с магнитных полос банковских карт.

Что же касается посягательства на собственность, то в данном случае имел место прямой неконкретизированный (неопределённый) умысел. Виновный, стремясь похитить как можно больше денежных средств, не мог наверняка знать, каким будет преступный результат: скольким потерпевшим и в какой сумме им будет причинён ущерб. Исходя из теории квалификации, при наличии неконкретизированного прямого умысла содеянное квалифицируется по фактически наступившим последствиям[2]. Если при неконкретизированном умысле последствия не наступили по причинам, не зависящим от воли виновного, то его общественно опасное поведение следует квалифицировать как приготовление (покушение) на причинение наименее опасного из всех желаемых вредных последствий[3]. Такое правило квалификации при неконкретизированном умысле вытекает из принципа необходимости толкования любого сомнения в пользу обвиняемого.

Если бы субъект преступления довёл свой умысел до конца, то потерпевшим стала бы кредитная организация при условии, что физические лица, со счетов которых были бы похищены денежные средства, успели бы воспользоваться правом, закреплённым в п.п. 11, 12 ст. 9 Федерального закона от 27 июня 2011 г. № 161 «О национальной платёжной системе»:

— в случае утраты электронного средства платежа и (или) его использования без согласия клиента клиент обязан направить соответствующее уведомление оператору по переводу денежных средств в предусмотренной

---

[1] Приговор Московского городского суда от 24.04.2013 по делу № 10-2268/2013 // СПС «КонсультантПлюс».

[2] Корнеева А. В. Теоретические основы квалификации преступлений: учеб. пособ. / Отв. ред. А. И. Рарог. 2-е изд. М.: Проспект, 2012. — С. 69–70.

[3] Там же. С. 96.

договором форме незамедлительно после обнаружения факта утраты электронного средства платежа и (или) его использования без согласия клиента, но не позднее дня, следующего за днём получения от оператора по переводу денежных средств уведомления о совершённой операции;

— после получения оператором по переводу денежных средств уведомления клиента в соответствии с ч. 11 ст. 9 оператор по переводу денежных средств обязан возместить клиенту сумму операции, совершённой без согласия клиента после получения указанного уведомления.

Вместе с тем, возможна ситуация, когда держатель карты своевременно не оповестил кредитную организацию о неправомерном списании денежных средств, следовательно потерпевшими будут и ООО АКБ «ХХХ», и сам держатель, которому кредитная организация вряд ли возместит похищенные денежные средства. Как видно, квалификация будет зависеть от конкретных обстоятельств дела и фактически наступивших последствий.

Предположим, что виновный достиг поставленной цели, неправомерно получил доступ к соответствующей информации, после чего используя «инкодер», персональный компьютер и соответствующее программное обеспечение, изготовил дубликаты банковских карт и, установив ПИН-коды, получил в банкомате денежные средства. В таком случае скопированная компьютерная информация будет являться средством совершения преступления, а ввод ПИН-кода — способом хищения.

В рассмотренном случае число преступных эпизодов зависело бы от числа потерпевших. Если в качестве потерпевшего признаётся исключительно кредитная организация, то содеянное образует единое продолжаемое преступление. В этом случае содеянное квалифицировалось бы по ч. 1 ст. 159.6 УК РФ, т. к. крупный размер хищения должен превышать 1 млн 500 тыс. руб. Однако если потерпевшими в силу приведённых выше причин окажутся и банк, и физические лица, то содеянное надлежит квалифицировать по совокупности преступлений, предусмотренных ст. 159^6 УК РФ. Поскольку же криминальная деятельность лица была пресечена на подготовительном этапе, то его ответственность по ч. 1 ст. 30 и ч. 1 ст. 159.6 УК РФ исключается (с учётом правил квалификации при неконкретизированном умысле) в силу ч. 2 ст. 30 УК РФ.

Если предположить, что неправомерный доступ к компьютерной информации охватывается таким признаком преступления, предусмотренного ст. 159^6 УК РФ, как иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации, и является способом совершения данного преступления (мошенничества в сфере компьютерной информации), такой доступ, при условии, что он повлёк указанные в ст. 272 УК РФ последствия, нуждается в самостоятельной уголовно-правовой оценке, поскольку данное деяние (хищение из банкомата) посягает на два различных объекта уголовно-правовой охраны.

Проблемы отграничения мошенничества в сфере компьютерной информации от кражи получили широкое распространение ввиду затруднений,

возникающих у правоприменителя при определении природы способа рассматриваемых преступлений.

Так, приговором Грачевского районного суда (Ставропольский край) от 13 июня 2013 г. Н. признана виновной в совершении преступления, предусмотренного ч. 1 ст. 159^6 УК РФ. Н., получив на мобильный телефон электронное сообщение посредством услуги «Мобильный банк» о доступном лимите денежных средств на не принадлежащем ей банковском счёте, открытом на имя Ш., используя сим-карту, зарегистрированную на имя Д., к которой ошибочно подключена услуга «Мобильный банк» «Сбербанка России», предоставляющая право распоряжаться денежными средствами, находящимися на расчётном счёту на имя Ш., путём ввода компьютерной информации в форме электрических сигналов — СМС-сообщения на номер 900, посредством телекоммуникационной сети оператора сотовой связи «Билайн» перечислила денежные средства, находившиеся на расчётном счёту Ш., на счёт, принадлежащей Н. сим-карты. Иная правовая оценка аналогичного деяния была дана одним из районных судов г. Белгорода.

С. получил сообщение на номер мобильного телефона, зарегистрированный на его имя, об остатке денежной суммы на банковской карте, находящейся в пользовании неизвестного ему лица. С использованием сайта компании сотовой телефонной связи в сети «Интернет» он перечислил сумму остатка денежных средств на счёт принадлежащей ему сим-карты, которую использовал в личных целях. Приговором Свердловского районного суда г. Белгорода от 13 июня 2013 г. С. признан виновным в совершении преступления, предусмотренного ч. 1 ст. 158 УК РФ. В ходе предварительного следствия действия С. были квалифицированы по совокупности ч. 1 ст. 158 и ч. 2 ст. 272 УК РФ. Суд исключил из обвинения ч. 2 ст. 272 УК РФ, мотивируя это тем, что «доказательств, подтверждающих позицию обвинения о наличии в действиях С. состава инкриминируемых преступлений, гособвинитель суду не представил. При предъявлении обвинения и в обвинительном заключении отсутствуют какие-либо признаки неправомерного доступа к охраняемой законом компьютерной информации и последствия в виде блокирования, модификации и копирования компьютерной информации, т. е. предъявленное в этой части С. обвинение не содержит признаков какого-либо самостоятельного состава преступления в сфере компьютерной информации, а действия подсудимого являются лишь способом совершения тайного хищения чужих денежных средств». Такое разночтение положений уголовного закона со стороны судов обусловлено спецификой предмета и способа преступного посягательства[1]. Полагаем всё же, что первое решение представляется более обоснованным, поскольку виновное лицо, понимая, что получает предназначенную не для него информацию, рас-

[1] *Иванченко Р. Б., Малышев А. Н.* Проблемы квалификации мошенничества в сфере компьютерной информации // Вестн. Воронеж. ин-та М-ва внутр. дел России. — 2014. — № 1. — С. 32–38.

поряжается ею, обманывая тем самым соответствующую кредитную организацию.

Наряду с вопросами отграничения смежных составов друг от друга в правоприменительной практике возникают трудности, связанные с толкованием понятий. Так, неоднозначно толкование понятия «иное вмешательство», присутствующего в ст. 159[6] УК РФ.

Пример «иного вмешательства» приводится в апелляционном определении Московского городского суда от 6 мая 2013 г. № 10-2076. Д. признан виновным в совершении девяти мошенничеств в сфере компьютерной информации, т. е. хищении чужого имущества путём иного вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации и информативно-телекоммуникационных сетей, группой лиц по предварительному сговору, с причинением значительного ущерба гражданину. А именно в том, что вступил в сговор с лицами, дело в отношении которых выделено в отдельное производство на хищение денежных средств со счетов граждан.

Получив информацию о счетах граждан, Д. изготавливал поддельные доверенности и получал дубликаты сим-карт и пароли. Далее, используя сим-карты и пароли, через электронную систему «Сбербанк-онлайн» путём перечисления на счета и банковские карты различных лиц завладевал денежными средствами[1].

В приговоре Подольского городского суда Московской области от 23 апреля 2013 г. по уголовному делу № 1-232/13 также рассматривается подобный вид мошенничества. На основании указанного приговора Г. осуждена по ч. 3 ст. 159.6 УК РФ за мошенничество в сфере компьютерной информации, т. е. хищение чужого имущества путём вмешательства в функционирование средств хранения, совершенное с использованием своего служебного положения, в крупном размере[2].

Как видим, из законодательных положений и приведённых судебных решений, в двух из которых подробно рассматривается «иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей», этот термин понимается неоднозначно. В одном случае своим содержанием охватывается неправомерный доступ к компьютерной информации, использование, распространение вредоносных компьютерных программ (ст.ст. 272, 273 УК РФ), а в другом — нет. Полагаем, что всё же понятие

[1] Апелляционное определение Московского городского суда от 06.05.2013 № 10-2076 // СПС «КонсультантПлюс».

[2] Приговор Подольского городского суда Московской области от 23.04.2013 по уголовному делу № 1-232/13 // Судебные решения РФ. Единая база данных решений судов общей юрисдикции Российской Федерации. [Электронный ресурс] — Режим доступа: http://www.gcourts.ru/case/ 14183520 (дата обращения: 28.02.2017).

иное вмешательство может охватывать указанные составы и должно трактоваться шире, чем лишь преступления в сфере компьютерной информации.

Суды стали широко применять ст. 159.6 УК РФ, когда действия виновного, начатые в сфере компьютерной информации, завершаются последующим изъятием или присвоением материальных предметов. Так, по ст. 159.6 УК РФ были осуждены П. и Е., работавшие менеджерами офиса продаж. По предварительному сговору, используя служебный компьютер, они произвели в электронных товарных накладных модификацию данных — замену артикулов дорогостоящей продукции на артикулы менее дорогой продукции. Получив, таким образом, возможность скрыть от учёта более дорогие товары, они похитили, как сказано в приговоре, товаров на сумму 344 тыс. 144 руб. из офиса продаж, и обратили в своё пользование[1].

Отдельные вопросы вызывает квалификация преступлений против собственности, совершаемых посредством сети «Интернет» и мобильной связи при наличии квалифицирующих признаков.

Интересен приговор Богдановичского городского суда Свердловской области в отношении П. и С., совершивших мошенничество в сфере компьютерной информации группой лиц по предварительному сговору. П., наряду с этим вменён квалифицирующий признак «с использованием служебного положения». Выявлено четыре эпизода преступной деятельности указанных лиц, совершённых при следующих обстоятельствах.

С., П. и неустановленное лицо вступили в предварительный преступный сговор на неправомерное завладение чужим имуществом, а именно на хищение денежных средств, принадлежащих ООО «Т2 Мобайл», путём мошенничества в сфере компьютерной информации. Неустановленное лицо, зарегистрированное в централизованной службе мгновенного обмена сообщениями интернет-мессенджера Telegram под интернет-псевдонимом, связалось посредством вышеуказанной социальной сети с С., которому сообщило о возможности незаконно обогатиться путём неправомерного доступа к охраняемой законом компьютерной информации и хищения денежных средств, принадлежащих ООО «Т2 Мобайл», посредством мошенничества в сфере компьютерной информации путём ввода и модификации компьютерной информации. После чего неустановленное лицо под интернет-псевдонимом известило С. о том, что оно располагает информацией о владельцах абонентских номеров, принадлежащих ООО «Т2 Мобайл», на лицевых счетах которых имеются денежные средства, а также о лице, являющемся сотрудником офиса продаж Tele2 и имеющем доступ к охраняемой законом компьютерной информации, содержащей персональные данные клиентов ООО «Т2 Мобайл» и их лицевых счетов. При этом неустановлен-

[1] Приговор Пресненского районного суда г. Москвы от 18.07.2013 по уголовному делу № 1-176/2013 / Судебные решения РФ. [Электронный ресурс] — Режим доступа: bsr/case/6511205 (дата обращения: 05.02.2017).

ное лицо сообщило С. о том, что в его обязанности, как участника преступной группы, будет входить передача сведений об абонентских номерах, на лицевых счетах которых имеются денежные средства, сотруднику офиса продаж ООО «Т2 Мобайл», а также перевод похищенных денежных средств на свой банковский счёт и их последующее распределение между участниками группы. Кроме того, неустановленное лицо сообщило С. о том, что для осуществления их совместного преступного умысла, ему необходимо связаться с менеджером офиса продаж Tele2 П. и вовлечь её в преступную группу, что С. и сделал. В ходе переписки С. сообщил П. о том, что в её обязанности, как участника преступной группы, будет входить написание заявлений от имени абонентов оператора сотовой связи ООО «Т2 Мобайл» на замену сим-карт с абонентскими номерами, на лицевых счетах которых имеются денежные средства, предоставленными ей неустановленным лицом под интернет-псевдонимом через С., а также производство модификации охраняемой законом компьютерной информации в автоматической биллинговой системе ООО «Т2 Мобайл» и перевод похищенных денежных средств на подконтрольные С. лицевые счета абонентских номеров. П. согласилась на данное предложение.

Неустановленное лицо под интернет-псевдонимом через Telegram сообщило С. сведения о наличии денежных средств, принадлежащих оператору сотовой связи ООО «Т2 Мобайл», в сумме <...> рублей на лицевом счёте абонентского номера, зарегистрированного на имя В., а также сведения о его полных паспортных данных, и сведения о наличии денежных средств, принадлежащих оператору сотовой связи ООО «Т2 Мобайл», в сумме <...> руб. на лицевом счёте абонентского номера, зарегистрированного на имя О., а также сведения о её полных паспортных данных.

С., в свою очередь, передал П. вышеуказанные сведения об абонентских номерах, их владельцах, а также о суммах, находящихся на лицевых счетах данных абонентских номеров.

П. на основании приказа о приёме работника на работу, трудового договора занимала должность менеджера офиса продаж Tele2 и в силу своего служебного положения была наделена полномочиями лица, осуществляющего организационно-распорядительные и административно-хозяйственные функции (обязанности) в коммерческой организации.

П., получив сообщение С. о наличии денежных средств на лицевых счетах указанных абонентских номеров, имея доступ к компьютерной программе WebDealer, содержащей персональные данные клиентов ООО «Т2 Мобайл» и данные их лицевых счетов, в нарушение требований Федерального закона Российской Федерации «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006, в отсутствие соответствующих заявлений абонентов оператора сотовой связи ООО «Т2 Мобайл» В. и О., под своей учётной записью зашла в программу WebDealer и произвела замену старых сим-карт на новые, имеющиеся в салоне сотовой

связи ООО «Т2 Мобайл». Затем, используя свой личный сотовый телефон Philips v387 и восстановленные сим-карты с абонентскими номерами оператора сотовой связи ООО «Т2 Мобайл», при помощи платёжной системы электронной системы платежей ЗАО «МОБИ.Деньги» осуществила перевод принадлежащих ООО «Т2 Мобайл» денежных средств с лицевого счета абонентского номера в сумме <...> рублей, с лицевого счета абонентского номера в сумме <...> рублей, всего на общую сумму <...> рублей. Похищенные денежные средства П. перевела на подконтрольные С. лицевые счета абонентских номеров оператора сотовой связи ПАО «ВымпелКом». Далее, С., путём СМС-команд произвёл перевод похищенных денежных средств в сумме <...> рублей с лицевых счетов абонентских номеров оператора сотовой связи ПАО «ВымпелКом» на свой лицевой счёт, открытый в Уральском банке ПАО «Сбербанк», по которому выпущена дебетовая банковская карта на его имя.

Затем П., С. и неустановленное лицо под интернет-псевдонимом распорядились денежными средствами по своему усмотрению, причинив ООО «Теле 2 Мобайл» материальный ущерб в сумме <...> рублей.

Аналогичным образом указанными лицами было совершено ещё два эпизода преступной деятельности, направленной на завладение чужим имуществом путём мошенничества в сфере компьютерной информации[1].

Необходимо отметить, что в данном случае суд счёл излишним вменение виновным лицам ст. 272 УК РФ. Полагаем решение обоснованно, поскольку доступ к компьютерной информации осуществляла только П., то данное обстоятельство исключается из действий остальных участников. Поскольку П. являлась менеджером по продажам и имела доступ к указанным сведениям, то, соответственно, такой доступ, в силу занимаемого П. положения, являлся правомерным, в связи с чем признаки состава преступления, предусмотренного ст. 272 УК РФ также отсутствуют.

В ряде случаев квалификация производится по общей, а не по специальной норме, исходя из обстоятельств дела, однако в совокупности с соответствующими составами преступлений в сфере компьютерной информации.

К примеру, М. и А. осуждены по нескольким эпизодам преступной деятельности, ответственность за которую предусмотрена ст.ст. 158, 159, 183, 272 УК РФ.

М., располагая информацией о возможности оформления через специалиста по работе с клиентами ООО «Доступный займ» — Б. договоров займа на имя лиц, ведущих антиобщественный образ жизни, вступил в преступный сговор с Б. и иным неустановленным в ходе следствия лицом на совершение хищений денежных средств, принадлежащих ООО «Доступный

[1] Приговор Богдановичского городского суда Свердловской области от 10.10.2016 № 1-158/2016 по делу С. и П. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/qBOwOSoZ5QgI/ (дата обращения: 31.03.2017).

займ» путём оформления займов в отсутствие, без ведома и разрешения заёмщика.

М. предоставлял Б. копии паспортов и страховых свидетельств пенсионного страхования, а также составленные им анкеты заёмщиков на имя С., Н., В., Б., а также анкету Ч. в обоснование их платёжеспособности.

Б., используя установленную на её рабочем компьютере программу, по предоставляемым ей М. документам составляла заведомо подложные договоры займа на указанных лиц и расходные кассовые ордера о получении заёмщиками денежных средств. Полученные от преступной деятельности денежные средства Б. передавала М., а тот, в свою очередь, часть из них в суммах от 500 до 1000 руб. передавал Б.

Так, М. совместно и по предварительному сговору с Б. и иным неустановленным в ходе предварительного расследования лицом совершил хищение денежных средств принадлежащих ООО «Доступный займ» в сумме 8 тыс. руб., причинив обществу материальный ущерб в указанной сумме.

Кроме того, М. совместно и по предварительному сговору с А. и иными неустановленными в ходе предварительного расследования лицами, располагая полученной при неустановленных в ходе предварительного расследования обстоятельствах информацией, об абонентском номере 1951134356 находящемся в пользовании П., и наличии на его лицевых счетах №….9017159, №….0402895, открытых в ОАО «Сбербанк России» денежных средств, решили совершить их хищение.

С указанной целью А., представившись по телефону П. сотрудником ОАО «Сбербанк России», сообщила ему о произошедшем в банке сбое баз данных, получив от потерпевшего сведения о его паспортных данных и месте регистрации. После чего А., в салоне связи восстановила сим-карты П., с номером, к которому подключена услуга «Мобильный банк» по банковским картам, находящимся в пользовании потерпевшего, передав её М., который, отправив СМС-сообщение со словом «Баланс» на номер 900, узнал сведения об остатках денежных средств на счетах П. После этого М. осуществил перевод денежных средств потерпевшего, аккумулировав их на одном счёте, а затем, используя услугу «Мобильный банк», направил СМС-сообщения на номер 900, осуществив перевод денежных средств в сумме 3 тыс. руб. с лицевого счета П., похитив их. Подобные операции М. повторил несколько раз, причинив потерпевшему ущерб на общую сумму 19 тыс. 950 руб. Затем денежные средства были обналичены А.

Кроме того, М. совместно и предварительному сговору с А. и иными неустановленными в ходе предварительного расследования лицами, являясь лицами, не имеющими права доступа к охраняемой законом компьютерной информации, представляющую собой банковскую и клиентскую тайну, предоставляемой услугой «Мобильный банк» ОАО «Сбербанк России», а также через систему «Сбербанк-онлайн», используя активную сим-карту оператора «Теле-2 Белгород», с абонентским номером, принадлежащим П., неза-

конно воспользовались услугой «Мобильный банк», предоставленной по данному телефонному номеру П., подключённому к лицевым счетам потерпевшего, открытых в ОАО «Сбербанк России» и необходимой для приёма, обработки и проведения комплекса операций, осуществляемых посредством мобильной связи и через систему «Сбербанк-онлайн». М. сформировал и направил СМС-сообщения, специального формата на номер 900, осуществив перевод денежных средств П. с лицевого счёта, на который им же ранее были переведены денежные средства П. в общей сумме 4 тыс. руб. с помощью системы «Сбербанк-онлайн»[1]. Остальные эпизоды преступной деятельности были совершены подобным образом.

Вместе с тем, позиция суда по квалификации подобных деяний по основному составу (ст. 159 УК РФ) вызывает большие сомнения. Нельзя также квалифицировать содеянное как кражу, поскольку имел место обманный способ завладения денежными средствами, сопряжённый с неправомерным доступом к компьютерной информации, что явно соответствует признакам состава преступления, предусмотренного ст. 159^6 УК РФ.

Вопросы, связанные с противодействием киберпреступлениям против собственности, в частности мошенничествам в сфере компьютерной информации, довольно часто возникают на международном уровне.

Необходимо отметить, что в законодательстве ряда зарубежных государств значительно усовершенствована регламентация уголовной ответственности за компьютерные преступления, используется чёткий понятийный аппарат и прописаны жёсткие санкции. За рубежом большое внимание уделяется обучению сотрудников правоохранительных органов и судей основам информационных технологий в целом и IT-безопасности в частности, что позволяет им самостоятельно выносить суждения по тем или иным аспектам компьютерных преступлений, не прибегая на первоначальном этапе квалификации к помощи экспертов и специалистов.

Санкции, предусмотренные уголовным законом Российской Федерации за преступления, совершаемые с помощью компьютерной информации, в том числе за компьютерное мошенничество, возможно, достаточно лояльны. Даже особо квалифицированный состав (ч. 4 ст. 159^6 УК РФ) по степени тяжести является тяжким (санкция предусматривает наказание до десяти лет лишения свободы). Вместе с тем, как показывает практика, лишение свободы в большинстве случаев не назначается. Наиболее распространённым видом наказания за подобные преступления является штраф либо условное осуждение.

В результате компьютерные злоумышленники несут ответственность, несоразмерную совершенным деяниям.

---

[1] Приговор Октябрьского районного суда г. Белгорода от 07.09.2015 № 1-198/2015 по делу М. и А. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/9ib9JSsB0UJR/ (дата обращения: 28.03.2017).

Показателен пример Е. Аникина и В. Плещука, взломавших компьютерную систему американской корпорации RBS World-Pay и похитивших с её счетов 10 млн долл. Указанные лица были признаны российским судом виновными, но приговорены лишь к условным срокам заключения. Тогда как за совершение общеуголовных преступлений, например, за хищение с нанесением ущерба на сумму 10—50 тыс. руб., осуждённые отбывают реальные сроки в местах лишения свободы[1].

Необходимо также акцентировать внимание на вымогательстве, совершённом с помощью компьютерной информации, поскольку судами в ряде случаев факт неправомерного доступа к компьютерной информации, если таковой имел место, не оценивается.

Так, Хасавюртовским городским судом Республики Дагестан А. осуждён по ч. 1 ст. 163 и ч. 2 ст. 128[1] УК РФ за совершение следующих деяний.

А. с использованием IP-адресов, зарегистрированный под именем «Фаир-Авердун», в сообществе на сайте «В Контакте» выложил для всеобщего просмотра посетителей сообщества фотографии Ю., а также сведения о частной жизни и комментарии, в которых содержатся сведения, порочащих честь и достоинство последней, с целью хищения чужого имущества путём вымогательства под угрозой дальнейшего распространения вышеуказанной информации. А. потребовал от Ю. денежные средства в сумме 10 тыс. руб. за удаление фотографий на счёт электронного кошелька Webmoney, которые были переведены последней[2]. Разумеется, в данном случае дополнительной квалификации по ст. 272 УК РФ. Однако в случае, когда виновный получил бы компрометирующие сведения путём неправомерного доступа к чужой информации, содеянное подлежало бы уголовно-правовой оценке и как неправомерный доступ к компьютерной информации.

Интересны факты квалификации действий виновных лиц по совокупности преступлений в сфере компьютерной информации, против собственности и в сфере экономической деятельности.

Так, Шебалинским районным судом Республики Алтай У. была осуждена по ст.ст. 183, 272 и 158 УК РФ.

У. незаконно собирала сведения, составляющие банковскую тайну, путём похищения документов; совершила кражу чужого имущества с причинением значительного ущерба гражданам; осуществила неправомерный доступ к охраняемой законом компьютерной информации, повлёкший мо-

---

[1] *Поддубная Е., Фернандес-Гонсалес Е.* Проблемы квалификации преступлений, связанных с хищением денежных средств в системах интернет-банкинга. [Электронный ресурс] — Режим доступа: http://www.group-ib.ru/index.php/212 (дата обращения: 12.03.2017).

[2] Приговор Хасавюртовского городского суда Республики Дагестан № 1-96/2015 от 6 мая 2015 г. по делу № 1-96/2015 [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/KWaHTTfQfcLw/ (дата обращения: 05.03.2017).

дификацию компьютерной информации, из корыстных заинтересованности при следующих обстоятельствах.

Являясь консультантом универсального дополнительного офиса отделения ОАО «Сбербанк России», без права допуска к банковской тайне У. собирала сведения, составляющие банковскую тайну путём похищения документов у 19-ти потерпевших клиентов банка.

Так, У., в обязанности которой входило предоставление консультационных услуг клиентам банка без права на получение и использование персональных данных клиентов и самостоятельного проведения операций, при предоставлении консультации клиенту Л. в ходе проведения им банковской операции по открытому на его имя счёту, без согласия Л., произвела на банкомате операцию по распечатыванию двух чеков ОАО «Сбербанк России», являющихся документами, содержащими сведения о номерах идентификатора пользователя, постоянного и одноразовых паролей, необходимых для получения доступа в сети «Интернет» к услуге автоматизированной системы обслуживания клиентов «Сбербанк-онлайн» интернет-сайта ОАО «Сбербанк России» по дистанционному управлению банковскими счетами, открытыми на имя Л.

После этого У. похитила распечатанные чеки, завладев содержащимися в указанных документах сведениями о номерах идентификатора пользователя, постоянного и одноразовых паролей, необходимыми для получения доступа к услуге системы «Сбербанк-онлайн» по дистанционному управлению банковским счётом, оформленным на имя Л. в ОАО «Сбербанк России», и отнесёнными ст. 857 Гражданского кодекса РФ и ст. 26 Федерального закона «О банках и банковской деятельности» к банковской тайне. Л. через специализированное программное обеспечение, введя ранее незаконно полученные ею номера идентификатора пользователя, постоянного и одного из одноразовых паролей банковской карты Л. «Маэстро» получила возможность незаконно использовать услугу системы «Сбербанк-онлайн» по дистанционному управлению банковским счётом, оформленным на имя Л. в ОАО «Сбербанк России», обслуживаемым по вышеуказанной банковской карте. Сразу же после этого У. незаконно осуществила в системе «Сбербанк-онлайн» безналичный перевод денежных средств в сумме 2 тыс. руб. с банковского счета, оформленного на имя Л. в ОАО «Сбербанк России», на банковский счёт, ранее ею открытый на своё имя в универсальном дополнительном офисе Горно-Алтайского отделения ОАО «Сбербанк России», т. е. тайно похитила принадлежащие У. денежные средства в сумме 2 тыс. руб. Аналогичные действия У. осуществила в отношении ещё 18-ти потерпевших[1].

[1] Приговор Шебалинского районного суда Республики Алтай от 21.06.2013 № 1/6-2013 по делу У. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/zVHRgrpIIpxC/ (дата обращения: 15.02.2017).

Интересно в данном случае то, что суд квалифицировал действия У. именно как кражу, но не как мошенничество в сфере компьютерной информации. Подобная позиция представляется неверной, поскольку имело место хищение денежных средств, совершённое путём ввода компьютерной информации в систему, другими словами, У. выполнила объективную сторону мошенничества в сфере компьютерной информации. Хищение же чеков в данном случае целесообразно расценивать как приготовление к совершению преступления.

Судебная практика по преступлениям против собственности, совершаемым посредством мобильной связи и сети «Интернет» весьма противоречива. Обусловлено это рядом факторов: резким ростом числа подобных преступлений при отсутствии у правоохранительных органов адекватных мер реагирования на них; относительной новизной уголовно-правовых норм, устанавливающих ответственность за преступления, связанные с информационными технологиями; отсутствием разъяснений Пленума Верховного суда РФ по вопросам квалификации таких деяний.

ЗАКЛЮЧЕНИЕ

Сегодня киберпреступность проникает во все сферы жизни человека, а имущественные отношения в первую очередь подвержены таким посягательствам. Для эффективной борьбы с ними, необходимо знать особенности таких преступлений.

Основным объектом группы преступлений против собственности, совершаемых посредством мобильной связи и сети «Интернет», следует признавать отношения, складывающиеся по поводу распределения и перераспределения материальных благ, влекущие основания для возникновения права пользования, владения или распоряжения имуществом, а дополнительным — нормальное функционирование информационных систем. Предметом указанных преступлений будет являться чужое имущество, в том числе безналичные денежные средства, электронные деньги и криптовалюта;

Объективная сторона преступлений против собственности, совершаемых посредством мобильной связи и информационно-телекоммуникационной сети «Интернет», всегда выражается в форме действия, характеризуется специфическим способом — воздействием на компьютерную информацию в целях хищения имущества или причинения имущественного ущерба, а также местом совершения преступления. Указанные преступления могут быть совершены как единолично, так и в соучастии. По способу конструкции объективной стороны составы данных преступлений являются преимущественно материальными, за исключением вымогательства;

Субъективная сторона посягательств на собственность, совершаемых посредством мобильной связи или сети «Интернет», выражена в форме прямого умысла, в ряде случаев по отношению к последствиям в виде уничтожения, блокирования, модификации либо копирования компьютерной информации возможен как прямой, так и косвенный умысел;

Субъект указанной категории преступлений общий, для субъекта вымогательства установлен пониженный возраст уголовной ответственности — с 14-ти лет.

Основными критериями отграничения посягательств на имущество от преступлений в сфере компьютерной информации выступают:

— объект посягательства (в обоих случаях объектом будет являться нормальный обмен компьютерной информацией, однако при посягательстве на собственность указанный объект будет выступать в качестве дополнительного);

— предмет преступления;

— особенности объективной стороны преступления (при посягательстве на имущество преступление в сфере компьютерной информации возможно рассматривать как часть способа преступления);

— субъективная сторона (при квалификации преступления необходимо установить направленность умысла).

Следует отграничивать составы преступлений против собственности, совершаемые с использованием сети «Интернет» или посредством мобильной связи, друг от друга, исходя из особенностей способа их совершения.

Квалификацию преступлений против собственности, совершаемых посредством сети «Интернет» или мобильной связи, уместнее начинать с признаков объективной стороны, следующим этапом должна быть квалификация по признакам субъективной стороны, затем — по признакам объекта и, наконец, по признакам субъекта преступления. В завершении необходимо установить наличие или отсутствие в действиях виновного квалифицирующих или особо квалифицирующих признаков.

Вместе с тем, наряду с первоначальной квалификацией по предложенному нами алгоритму, при окончательной квалификации всё же необходимо ориентироваться на заключения всех необходимых экспертиз, а также заключения специалистов в области компьютерных технологий.

Несмотря на противоречия судебной практики по преступлениям против собственности, совершаемым посредством мобильной связи и сети «Интернет», при их квалификации необходимо строго следовать букве закона, ориентируясь при этом на имеющиеся решения судов с учётом их критического анализа.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Официальные документы:

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в посл. ред.) // СЗ РФ. — 1996. — № 25. — Ст. 2954.

2. Об информации, информационных технологиях и защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ (в посл. ред.) // Рос. газ. — 2006. — 29 июля. — № 165.

3. Об утверждении Доктрины информационной безопасности Российской Федерации : указ президента Рос. Федерации от 5 дек. 2016 г. № 646 // СЗ РФ. — 2016. — № 50. — Ст. 7074.

4. О некоторых вопросах применения судами законодательства об ответственности за преступления против собственности: постановление Пленума Верховн. Суда Рос. Федерации от 25 апр. 1995 г. № 5 // Рос. газ. — 1995. — 31 мая.

5. Информационное сообщение Росфинмониторинга «Об использовании криптовалют» // СПС «КонсультантПлюс».

Документальные материалы:

6. Апелляционное определение Московского городского суда от 06.05.2013 № 10-2076 // СПС «КонсультантПлюс».

7. Данные ЦСИ ГИАЦ МВД России.

8. Обзор практики рассмотрения уголовных дел о мошенничестве, присвоении и растрате (статьи 159, 159.1–159.6, 160 УК РФ) судами Пензенской области в 2014–2015 гг. [Электронный ресурс] — Режим доступа: http://www.oblsud.penza.ru/item/1220/ (дата обращения: 09.12.2016).

9. Приговор Промышленного районного суда г. Самары от 4 окт. 2016 г. по делу № 1-206/2016. [Электронный ресурс] — Режим доступа: http://www.sudact.ru (дата обращения: 12.12.2016).

10. Приговор Братского городского суда Иркутской области № 1-487/2016 от 08.11.2016 по делу А. [Электронный ресурс] — Режим доступа: http://www.sudact.ru (дата обращения: 30.11.2016).

11. Приговор Знаменского районного суда Омской области № 1-35/2016 от 03.11.2016 по делу А. [Электронный ресурс] — Режим доступа: http://www.sudact.ru (дата обращения: 30.11.2016).

12. Приговор Можгинского районного суда Удмуртской Республики № 1-162/2010 от 13.08.2010 по делу М. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/8h4NgygCHCUR/ (дата обращения: 02.12.2016).

13. Приговор Каспийского городского суда Республики Дагестан № 1-87/2015 от 12.05.2015 по делу Р. [Электронный ресурс] — Режим доступа: http://www.sudrf.ru (дата обращения: 15.10.2016).

14. Приговор Нижегородского городского суда № 1-29/2015 от 10.09.2015 по делу А. [Электронный ресурс] — Режим доступа: http://www.sudact.ru (дата обращения: 15.10.2016).

15. Приговор Самарского районного суда г. Самары № 1-156/2015 от 03.08.2015 по делу Д. и К. [Электронный ресурс] — Режим доступа: http://www.sudact.ru (дата обращения 02.12.2016).

16. Приговор Советского районного суда г. Улан-Удэ (Республика Бурятия) № 1-715/2015 от 22.09.2015 по делу Б. [Электронный ресурс] — Режим доступа:http://sudact.ru/regular/doc/x60NkKWhBNx3 (дата обращения: 01.12.2016).

17. Приговор Железнодорожного районного суда г. Читы (Забайкальский край) № 1-166/2016 от 22.04.2016 по делу Г. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/qVBsoHNvRYrQ/ (дата обращения: 06.12.2016).

18. Приговор Шелеховского городского суда Иркутской области от 10.02.2015 № 1-12/2015 по делу А. [Электронный ресурс] — Режим доступа: http://sudact.ru (дата обращения: 06.03.2017).

19. Приговор Братского городского суда Иркутской области от 23.03.2015 по делу № 1-130/2015. [Электронный ресурс] — Режим доступа: http://sudact.ru (дата обращения: 06.03.2017).

20. Приговор Пролетарского районного суда г. Тулы от 24.03.2016 № 1-32/2016 по делу Р. и Л. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/V7owrOu68Cr/ (дата обращения: 11.03.2017).

21. Приговор Железнодорожного районного суда г. Читы (Забайкальский край) № 1-465/2015, 1-64/2016 от 29.04.2016 по делу А. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/Sdk2JBd3c3ru/ (дата обращения: 09.12.2016).

22. Приговор Сарапульского городского суда Удмуртской Республики от 07.10.2016 № 1-256/16 по делу К. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/p5StY3oz79UV/ (дата обращения: 10.03.2017).

23. Приговор Железнодорожного районного суда г. Орла от 30.05.2016 № 1-20/2016 по делу Б. // [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/66yDzpTT6qJx/ (дата обращения: 11.03.2017).

24. Практика районных судов г. Москвы. [Электронный ресурс] — Режим доступа: http://urist-msk.pro/pp/cher_163_2.html (дата обращения: 17.03.2017).

25. Приговор Дзержинского районного суда г. Новосибирска от 21.12.2012 № 1-705/12 по делу С. [Электронный ресурс] — Режим доступа: https://rospravosudie.com/court-dzerzhinskij-rajonnyj-sud-g-novosibirska-novosibirskaya-oblast-s/act-425470944/ (дата обращения: 18.03.2017).

26. Приговор Кировского районного суда г. Астрахани от 08.09.2015 № 1-409/2015 по делу Д. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/ZE0dnyLDpJQQ/ (дата обращения: 19.03.2017).

27. Приговор Люблинского районного суда г. Москвы от 07.04.2014 № 1-1/2014. [Электронный ресурс] — Режим доступа: http://sudact.ru/ regular/ doc/IgF7Z3v8VIgZ/ (дата обращения: 09.03.2017).

28. Постановление Президиума Алтайского краевого суда от 03.09.2013 по делу № 44у224/13 // СПС «КонсультантПлюс».

29. Приговор суда г. Дагестанские Огни Республики Дагестан по делу № 1-28/2013. [Электронный ресурс] — Режим доступа: http://www.gcourts.ru/ case/22900134 (дата обращения: 01.03.2017).

30. Приговор Московского городского суда от 24.04.2013 по делу № 10-2268/2013 // СПС «КонсультантПлюс».

31. Приговор Братского районного суда Иркутской области № 1-122/2015 от 15.05.2015 по делу Г. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/qVBsoHNvRYrQ/ (дата обращения: 06.12.2016).

32. Приговор Подольского городского суда Московской области от 23.04.2013 по уголовному делу № 1-232/13 // Судебные решения РФ. Единая база данных решений судов общей юрисдикции Российской Федерации. [Электронный ресурс] — Режим доступа: http://www.gcourts.ru/case/14183520 (дата обращения: 28.02.2017).

33. Приговор Пресненского районного суда Москвы от 18.07.2013 № 1-176/2013 / Судебные решения РФ. [Электронный ресурс] — Режим доступа: http://www.bsr/case/6511205 (дата обращения: 05.02.2017).

34. Приговор Самарского районного суда Самары 05.03.2014 № 1-34/2014 / Судебные решения РФ. [Электронный ресурс] — Режим доступа: http:// www.gcourts.ru/case/23839448 (дата обращения: 15.02.2017).

35. Приговор Богдановичского городского суда Свердловской области от 10.10.2016 № 1-158/2016 по делу С. и П. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/qBOwOSoZ5QgI/ (дата обращения: 31.03.2017).

36. Приговор Первомайского районного суда Оренбургской области от 08.07.2016 № 1-58/2016 по делу С. Е. и С. О. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/niLXZB6A8dgR/ (дата обращения: 31.03.2017).

37. Приговор Октябрьского районного суда г. Белгорода от 07.09.2015 № 1-198/2015 по делу М. и А. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/9ib9JSsB0UJR/ (дата обращения: 28.03.2017).

38. Приговор Хасавюртовского городского суда Республики Дагестан № 1-96/2015 от 6 мая 2015 г. по делу № 1-96/2015 [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/KWaHTTfQfcLw/ (дата обращения: 05.03.2017).

39. Приговор Трусовского районного суда г. Астрахани от 27.09.2016 № 1-176/2016 по делу Н. и М. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/3eGvCqZG7454/ (дата обращения: 22.03.2017).

40. Приговор Шебалинского районного суда Республики Алтай от 21.06.2013 № 1/6-2013 по делу У. [Электронный ресурс] — Режим доступа: http://sudact.ru/regular/doc/zVHRgrpIIpxC/ (дата обращения: 15.02.2017).

41. Статистические данные МВД России: [Электронный ресурс] — Режим доступа: http:www.mvd.ru/deyatelnost/statistics (дата обращения: 03.03.2017).

42. Статистические данные Информационного центра ГУ МВД России по Иркутской области.

Учебники, учебные пособия, монографии, статьи, научные публикации

43. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность. — М., Юриспруденция, 2015. — 160 с.

44. Безверхов А. Г. Имущественные преступления. — Самара, 2002. — 359 с.

45. Болсуновская Л. М. Мошенничество в сфере компьютерной информации: анализ судеб. практики // Угол. право. — 2016. — № 2. — С. 39–43.

46. Бойцов А. И. Преступления против собственности. — СПб.: Юрид. центр ПРЕСС, 2002. — 775 с.

47. Векленко В. В. Квалификация хищений: монография. — Омск, 2001. — 256 с.

48. Вишнякова Н. В. Объект и предмет преступлений против собственности: дис. … канд. юрид. наук. — Омск, 2003. — 210 с.

49. Гражданское право: учеб.: в 2 т. / под ред. В. П. Мозолина, А. И. Масляева. — М., 2007. — Т. 1. — 719 с.

50. Гражданское право: учеб.: в 3 т. / под ред. А. П. Сергеева, Ю. К. Толстого. — М., 2003. — Ч. 1. — 880 с.

51. Дашян М. С. Право информационных магистралей: вопрос правового регулирования в сети «Интернет». — М.: Волтерс Клувер, 2007. — 275 с.

52. Евдокимов К. Н. Проблемы квалификации и предупреждения компьютерных преступлений: монография. — Иркутск: Ирк. юрид. ин-т (филиал) Акад. Ген. прокуратуры РФ, 2009. — 171 с.

53. Иванченко Р. Б., Малышев А. Н. Проблемы квалификации мошенничества в сфере компьютерной информации // Вестн. Воронеж. ин-та М-ва внутр. дел России. 2014. — № 1. — С. 32–38.

54. Киселёв А. К. Киберпреступность — взгляд из Европы // Библиотека криминалиста. — 2013. — № 5 (10). — С. 310–315.

55. Клепицкий И. А. Недвижимость как предмет хищения и вымогательства // Гос-во и право. — 2000. — № 12. — С. 13–15.

56. Комментарий к уголовному кодексу Российской Федерации / С. А. Боженок, Ю. В. Грачёва, Л. Д. Ермакова и др.; отв. ред. А. И. Рарог. — 10-е изд., перераб. и доп. — М.: Проспект, 2015. — 1056 с.

57. Корнеева А. В. Теоретические основы квалификации преступлений: учеб. пособ. / Отв. ред. А. И. Рарог. — 2-е изд. — М.: Проспект, 2012. — 110 с.

58. Косенков А. Н., Чёрный Г. А. Общая характеристика психологии киберпреступника // Криминол. журнал БГУЭП. — 2012. — № 3 (21). — С. 87–94.

59. Кочои С. М. Уголовное право. Общая и Особенная части. Краткий курс: учеб. — М., 2010. — 513 с.

60. Лопатина Т. М. Проблемы формирования уголовно-правового способа борьбы с компьютерным мошенничеством // Библиотека криминалиста. — 2013. — № 5. — С. 34–40.

61. Неклюдов Н. А. Руководство к Особенной части русского уголовного права: в 2 т. — СПб., 1876. Т. 2: Преступления и проступки против собственности. — 555 с.

62. Питулько К. В., Караковцев В. В. Уголовное право. Особенная часть. — СПб., 2010. — 256 с.

63. Простосердов М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. … канд. юрид. наук. — М., 2016. — С. 232.

64. Простосердов М. А. Мошенничество, совершаемое в киберпространстве, и его виды / М. А. Простосердов // Актуальные проблемы теории и практики применения уголовного закона: сб. мат-лов науч.-практ. конф. / Под ред. А. В. Бриллиантова и Ю. Е. Пудовочкина. — М.: РГУП, 2015. — С. 334–351.

65. Российское уголовное право. Особенная часть / Под ред. В. Н. Кудрявцева, А. В. Наумова. — М., 1997. — 540 с.

66. Уголовное право России. Особенная часть: учеб. / Под ред. В. П. Ревина. — М., 2010. — 330 с.

67. Уголовное право Российской Федерации. Особенная часть: учеб. / Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. — М., 2009. — 634 с.

68. Фатьянов А. А. Правовой анализ категории «электронные денежные средства» в российском законодательстве // Гражд. о-во в России и за рубежом. 2014. № 3 // СПС «Консультант плюс».

69. Хилюта В. В. Хищение с использованием компьютерной техники или компьютерное мошенничество? // Библиотека криминалиста. — 2013. — № 5 (10). — С. 23–27.

70. Шарапов Р. Д. Актуальные вопросы квалификации новых видов мошенничества // Проблемы квалификации и расследования преступлений, подследственных органам дознания: материалы всерос. науч.-практ. конф. Тюмень: Тюм. ин-т повышения квалификации. — 2013. — С. 3–5.

71. Шульга А. В. Объект и предмет преступлений против собственности в условиях рыночных отношений и информационного общества. — М., 2007. — 62 с.

Электронные ресурсы:

72. Концепция Стратегии кибербезопасности Российской Федерации. [Электронный ресурс] — Режим доступа:http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 01.12.2016).

73. Поддубная Е., Фернандес-Гонсалес Е. Проблемы квалификации преступлений, связанных с хищением денежных средств в системах интернет-банкинга. [Электронный ресурс] — Режим доступа: http://www.group-ib.ru/index.php/212 (дата обращения: 12.03.2017).

Учебное издание

Бархатова Екатерина Николаевна

ОСОБЕННОСТИ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ ПРОТИВ СОБСТВЕННОСТИ, СОВЕРШАЕМЫХ ПОСРЕДСТВОМ МОБИЛЬНОЙ СВЯЗИ И СЕТИ «ИНТЕРНЕТ»

Редактор
А. В. Андреев

Подписано в печать 21.08.17 Формат 60 х 84/16
Усл. печ. л. 5,0 Тираж 100 экз. Заказ № 44

НИиРИО ФГКОУ ВО «Восточно-Сибирский институт МВД России»,
ул. Лермонтова, 110