УДК 343

ПРАКТИЧЕСКИЕ ПРОБЛЕМЫ ЗАЩИТЫ ПРАВ ПОТЕРПЕВШИХ ПРИ ПРИВЛЕЧЕНИИ К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ КИБЕРПРЕСТУПНИКОВ

Филимонов С.А.[1], Олейников А.А.[2]

[1] ФГБОУ ВПО «Кубанский государственный аграрный университет», Краснодар, Россия (350044 г. Краснодар, ул. Калинина, 13), e-mail: filinlow@rambler.ru;
[2] ГСУ ГУ МВД РФ по Краснодарскому краю, Краснодар, Россия (350063 г. Краснодар, ул. Красноармейская, 12), e-mail: filinlow@rambler.ru.

В настоящее время в результате научного прогресса увеличилось количество киберпреступлений. В связи с высокой латентностью данного вида преступлений многие потерпевшие вообще не регистрируют факты совершения этого вида преступлений, большое количество киберпреступлений даже не выявляется, не говоря об их расследовании и привлечении преступников к уголовной ответственности. Одной из причин такого поведения потерпевших по данной категории преступлений является тот факт, что вероятность поймать киберпреступника минимальна, а время, потраченное на подачу заявления в порядке ст. 141 УПК РФ и дачу объяснения при проведении проверки по ст. 144 УПК РФ, никем материально компенсировано не будет, как и ущерб, причиненный киберпреступлением. Эти факты идут в прямом противоречии с положениями, закрепленными в ст. 52 Конституции РФ и работой Общественной палаты РФ по подготовке проектов нормативно – правовых актов об усилении защиты прав потерпевших. Авторы приводят конкретные проблемы, возникающие у правоохранительных органов в отношении защиты прав потерпевших, пострадавших от киберпреступлений и вносят свои предложения по совершенствованию действующего уголовного законодательства в этой части.
Ключевые слова: потерпевший, киберпреступность, хищение, кража, мошенничество.

PRACTICAL PROBLEMS OF PROTECTION OF THE RIGHTS OF VICTIMS AT BRINGING TO CRIMINAL LIABILITY OF CYBERCRIMINALS

Filimonov S.A.[1], Olejnikov A.A.[2]

[1] Kuban state agrarian university», Krasnodar, Russia (350044 Krasnodar, street of Kalinin, 13), e-mail: filinlow@rambler.ru;
[2] The main investigatory management of central administrative board of the Ministry of Internal Affairs of the Russian Federation across Krasnodar territory, Krasnodar, Russia (350063 Krasnodar, street Krasnoarmejsky, 12), e-mail: filinlow@rambler.ru.

Now as a result of scientific progress the quantity of cybercrimes has increased. In connection with high abeyance the given kind of crimes many victims at all do not register the facts of fulfillment of this kind of crimes, a considerable quantity of cybercrimes does not come to light at all, without speaking about their investigation and attraction of criminals to a criminal liability. One of the reasons of such behavior of victims on the given category of crimes is that fact that the probability to catch the cybercriminal is minimum, and time spent for filing of application as item 141 the criminal procedural code of the Russian Federation and an explanation summer residence at check carrying out under item 144 the criminal procedural code of the Russian Federation anybody will not be financially compensated, as well as a damage caused by a cybercrime. These facts go in the direct contradiction with the positions fixed in item 52 of the Constitution of the Russian Federation and work of Public chamber of the Russian Federation on preparation of projects standard - legal certificates about strengthening of protection of the rights of victims. Authors result the concrete problems arising at law enforcement bodies concerning protection of the rights of victims, suffered from cybercrimes and make the offers on perfection of the operating criminal legislation in this part
Keywords: victim, cybercriminality, plunder, theft, swindle.

Согласно требованиям ст. 52 Конституции РФ права потерпевших от преступлений и злоупотреблений властью охраняются законом. Государство обеспечивает потерпевшим доступ к правосудию и компенсацию причиненного ущерба. В силу требований ч. 1 ст. 2 УК РФ задачами уголовного кодекса РФ являются, в том числе, охрана прав и свобод человека и гражданина, собственности от преступных посягательств. Серьезную работу по разработке проектов новых нормативно – правовых актов по защите прав потерпевших проводят

доверенное лицо Президента РФ, председатель правления МПОО «Сопротивление», член Общественной палаты РФ Ольга Костина, а также известные ученые-юристы и другие общественные организации. О необходимости дополнительной защиты прав потерпевших указывал и руководитель Следственного Комитета РФ. Налицо стремление правоприменителей обратить внимание на необходимость сделать защиту прав и законных интересов потерпевших от преступлений более эффективной, перевести соответствующие уголовно-правовые нормы, которые имеют декларативный характер, в разряд эффективно действующих, направленных на реализацию потерпевшим своих полномочий по реальному возмещению последним вреда, причиненного противоправным преступным деянием. Вместе с тем, при привлечении к уголовной ответственности киберпреступников, правоохранительные органы сталкиваются с целым рядом проблем по обеспечению прав потерпевших по этой категории преступлений.

Цель исследования

В данной статье мы предпримем попытку дальнейшего теоретического познания института защиты прав потерпевших, пострадавших от киберпреступлений, разработки на основе достижений юридической науки и обобщения следственной практики предложений по совершенствованию уголовного материального права и деятельности правоохранительных органов по применению указанного института.

Материал и методы исследования, результаты исследования и их обсуждение

В настоящее время идет широкомасштабное формирование глобального информационного общества, при котором проблема обеспечения безопасности информации выходит на первый план. При этом от правоохранительных органов требуется грамотное и своевременное противодействие преступным посягательствам в сфере обращения цифровой информации.

В.Б. Завидов, комментируя законодательство об ответственности за совершение компьютерных преступлений, отмечает, что «парадоксально, но законодатель как бы не замечает того, что постоянно совершенствующиеся экономические отношения настоятельно требуют изменения уголовного законодательства» [5]. По данным ЗАО «Лаборатория Касперского», каждый день проявляется порядка 125 тысяч вредоносных объектов (файлов), и злоумышленники становятся все более изобретательными. За последние годы около 90 % российских компаний фиксировали инциденты в сфере IT-безопасности. При этом более половины опрошенных специалистов признали факт потери данных в результате заражения вредоносным программным обеспечением (ПО). Наиболее часто IT-специалисты сталкиваются с вирусами. В список актуальных угроз также входят спам, фишинг, сетевые атаки на инфраструктуру бизнес-структур, включая DDos-атаки. Чаще всего инциденты в области IT-безопасности приводят к потере данных, касающихся платежей (13 %),

интеллектуальной собственности (13 %), клиентских баз (12 %), информации о сотрудниках (12 %) [12]. Сегодня в особом фокусе киберприцела находятся государственные и коммерческие структуры, занимающиеся разработкой оружия и боеприпасов, крупные научно-технические и исследовательские центры и институты, финансовые структуры. К зоне пристального внимания и высокого риска относятся компании, занимающиеся информационной безопасностью, энергетические, добывающие и транспортные структуры (отрасли), а также крупные интернет-сервисы. При этом отмечается расширение ареала объектов кибератак. Помимо стран Западной Европы и США, в ареал все шире «втягиваются» государства Юго-Восточной Азии, Восточной Европы и Ближнего Востока. При этом возрастает количество хакерских атак на различные государственные структуры. В связи с динамичным и масштабным ростом киберугроз и киберпреступлений, причиняемого ими ущерба юридическим и физическим лицам, в том числе, поставщикам услуг, такие угрозы и преступления представляют серьезнейшую проблему для общества, а борьба с ними является актуальной и стратегически важной задачей для правоохранительных органов, особенно в части, касающейся реализации мер, направленных на эффективное противодействие росту киберпреступлений, своевременное установление лиц, совершивших преступные деяния, и, конечно, получение доказательств, подтверждающих совершение правонарушения. По сути дела, глобальное киберпространство и действующие в нем разветвленные элементы инфраструктуры Интернет, мобильных сетей связи (телекоммуникации) служат наиболее востребованными злоумышленниками средствами совершения преступлений, как для хакеров, так и для различного рода мошенников, террористов, торговцев «живым» товаром, наркотиками и т.п. Отметим, что проблемам криминологического и уголовно-правового предупреждения киберпреступности в России в последние два десятилетия определенное внимание уделяется. Однако время неумолимо и крайне быстро идет вперед. Сегодня злоумышленниками все чаще используются новые электронные способы и средства, например, мобильные системы связи, возможности интернет-банкинга [11].

Как обоснованно указывает С.Д. Бражник, в Уголовном кодексе Российской Федерации отсутствует специальная норма, предусматривающая ответственность за совершение «компьютерного хищения», и правоприменительная практика исходит из того, что хищения, совершаемые с использованием компьютерной техники, в ряде случаев рассматриваются либо как мошенничество, либо как кража по признаку незаконного проникновения в помещение или иное хранилище. Кроме этого, такого рода противоправные действия дополнительно влекут уголовную ответственность по ст. 272 УК РФ [2]. В.В. Хилюта справедливо замечает, что не вполне обоснованно рассматривать такого рода хищения, как кражу, ввиду того, что в компьютерной системе не хранятся вещи, денежные средства или иное имущество, на которые посягает преступник, в компьютерной системе хранится информация об этом имуществе или

его передвижении. Если виновное лицо проникает в компьютерную систему с целью завладения денежными средствами либо иного имущества, то делает оно это путем манипуляций с программами, данными, либо техническими средствами. Таким образом, лицо для совершения имущественного преступления умышленно искажает либо вносит ложные данные в компьютерную систему, манипулирует с программами, данными, аппаратной частью ЭВМ, обрабатывающими информацию о передвижении имущества, и тем самым добивается получения разрешения на использование имущества [10].

Предметом хищения могут выступать и безналичные деньги, хранящиеся на счетах в банках и кредитных организациях. Например, С., Г. и Я. группой лиц по предварительному сговору, используя поддельные документы, снимали денежные средства с расчетных счетов предприятий городов Брянска, Сургута, Орска, Питкяранта (Республика Карелия) и перечисляли их на расчетный счет ООО «Энергоавтоматика» в Брянске. Затем соучастники преступления обналичивали эти денежные средства, производя по подложным платежным поручениям их перечисление со счета ООО «Энергоавтоматика» на расчетный счет Г., который снимал деньги, и они затем распределялись между участниками преступной группы. По приговору Советского районного суда г. Брянска от 22 марта 2002 г. указанные действия Я. были квалифицированы по ч. 3 ст. 159 УК и ч. 3 ст. 174 УК, а С. и Г. – по этим же статьям и дополнительно по ч. 2 и ч. 3 ст. 327 УК. Судебная коллегия по уголовным делам Брянского областного суда, рассмотрев данное дело по кассационной жалобе осужденного, согласилась с квалификацией преступлений названных выше лиц, исключив из обвинения ст. 174 УК. Использование расчетного счета, на который по поддельным платежным поручениям перечислялись чужие денежные средства, в следственно-судебной практике рассматривается как хищение, совершенное путем обмана. Поскольку расчеты в соответствии со ст. 140 ГК могут осуществляться как в наличной, так и в безналичной форме, то денежные суммы, находящиеся на банковских счетах, – это такое же платежное средство, как и наличные деньги. Следовательно, они могут считаться предметом хищения [4].

Сотрудники государственных органов, к сожалению, не приводят неутешительной статистики высокой латентности киберпреступлений. Мы согласны с М.В. Старичковым, который называет уровни латентности порядка 99,7 % по ст. 272 УК РФ и 99,8 % по ст. 273 УК РФ как для всех преступлений в сфере компьютерной информации, так и для преступлений, совершенных посредством Интернета, хотя замечает, что полученные данные вряд ли могут претендовать на абсолютную достоверность [8]. По мнению Т.Л. Тропиной, высокая искусственная латентность компьютерных преступлений обусловлена также тем, что многие организации разрешают конфликт своими силами, поскольку убытки от расследования могут оказаться выше суммы причиненного ущерба. Например, изъятие файлового сервера для проведения экспертизы может привести к остановке работы на срок до двух месяцев, что

неприемлемо ни для одной организации [9]. Как обоснованно указывает С.В. Воронцова, изготовление или сбыт поддельных платежных карт, незаконное получение информации об эмитированных платежных картах, а также о реквизитах и кодах платежных карт – это приготовление к совершению противоправных действий (ст. 30 УК РФ). Но ответственность за подготовку может наступить только при совершении тяжких и особо тяжких преступлений. Однако определять тяжесть подготавливаемого преступления достаточно сложно. Существует точка зрения, что списание денежных средств со счета владельца банковской карты с использованием поддельной карты образует состав преступления, предусмотренного ст. 272 Уголовного кодекса РФ, так как фактически происходит изменение компьютерной информации по счету владельца карты (уменьшение баланса по счету). В то же время необходимо принимать во внимание субъективную сторону преступления. Умысел преступника направлен не на получение охраняемой законом компьютерной информации с целью ее уничтожения, блокирования или модификации, а на получение денежных средств либо товаров в торговой организации за счет денежных средств на банковском счете. В ряде случаев эти деяния можно квалифицировать по ст. 183 Уголовного кодекса РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну».

Проблемой является также то, что потерпевшим по данной категории дел будет не пользователь карты, а банк-эмитент. Это влечет за собой сокрытие преступлений, т.к. в настоящее время в условиях жесткой конкуренции зачастую банки, боясь антирекламы и утечки коммерческой информации, скрывают факты хищений собственных и вверенных им денежных средств и иных злоупотреблений, что нередко ставит их на грань разорения и в итоге ущемляет права и интересы граждан, дестабилизирует экономику страны в целом [3].

Как обоснованно указывает А.А. Комаров, высокая латентность и безнаказанность киберпреступников может повлечь переход традиционных форм мошенничества в интернет и приведет к снижению выявляемости и раскрываемости деяний, совершенных данным способом [6]. В этом случае уже ничто не зависит от нашей внимательности, осторожности или предусмотрительности. Бывает, что в сговор с мошенниками вступают те люди, которым добраться до наших кредитных карт и так очень просто: служащие банков, например. Это случается очень редко, но от таких случаев не застрахован никто. Но страдают не только владельцы карточек. Страдают и крупные фирмы, магазины, банки. Причем здесь убытки уже исчисляются сотнями тысяч долларов. А иногда миллионами. По некоторым данным, на сегодняшний день насчитывается около 30 видов незаконных операций с карточками через Всемирную паутину. Наиболее распространенные из них – оплата несуществующими картами, создание фальшивых виртуальных магазинов, электронное воровство, фальшивая оплата в игорных заведениях [1]. Данные сведения свидетельствуют о серьезных проблемах

правоохранительных органов в борьбе с подавляющим большинством киберпреступлений (и прежде всего компьютерного мошенничества), которые даже не выявляются, не говоря об их расследовании и привлечении преступников к уголовной ответственности. Потерпевшие по данной категории преступлений вряд ли захотят обращаться в правоохранительные органы, поскольку вероятность поймать киберпреступника минимальна, а время, потраченное на подачу заявления в порядке ст. 141 УПК РФ и дачу объяснения при проведении проверки по ст. 144 УПК РФ никем материально компенсировано не будет, как и ущерб, причиненный киберпреступлением.

При расследовании киберпреступлений возникают и проблемы с установлением потерпевшего. Так, в 2013–2014 годах в СЧ ГСУ ГУ МВД РФ по Краснодарскому краю окончено производством уголовное дело, возбужденное 31.05.2012 года по признакам состава преступления, предусмотренного ч.3 ст.30, п. «а» ч.2 ст.158 УК РФ в отношении У., М. и С. Так, согласно разработанному плану, в функции У входило создание условий для зачисления по безналичному расчету денежных средств, похищенных со счетов банковских карт, владельцы которых не осведомлены о преступных намерениях участников сговора, а именно: предоставление реквизитов расчетного счета, открытого им 13.03.2012 года в филиале банка, получение ПОС-терминала оплаты, необходимого для осуществления платежных операций с использованием указанных карт, а также обеспечение возможности распорядиться похищенными денежными средствами, поступившими на его расчетный счет.

В функции С. входило собирание иным незаконным способом сведений, содержащих банковскую тайну путем приобретения в сети «Интернет» данных магнитных полос чужих расчетных банковских карт, держатели которых не осведомлены о преступных намерениях участников сговора, осуществление их записи на пластиковые карты с магнитными полосами, с использованием компьютерной программы, заведомо предназначенной для несанкционированного копирования компьютерной информации, то есть создание условий для осуществления платежных операций по списанию денежных средств со счетов банковских карт, держатели которых не осведомлены о преступных намерениях участников сговора.

В функции М. входило, под видом оплаты туров через предоставленный У. ПОС-терминал оплаты, при помощи дубликатов чужих расчетных банковских карт, осуществление платежных операций по перечислению чужих денежных средств на расчетный счет, принадлежащий индивидуальному предпринимателю У. В дальнейшем, участники этого преступления намеревались обналичить похищенные ими чужие денежные средства, зачисленные под видом оплаты туров на расчетный счет индивидуального предпринимателя У. и распределить их между собой. Действуя в соответствии с разработанным планом и согласно отведенной ему функции в совершении преступления, У. в целях обеспечения возможности зачисления похищенных денежных средств на свой расчетный счет

зарегистрировал у себя в офисе, переносной ПОС-терминал оплаты банка модели VeriFone VX 510. Далее, во исполнение преступного плана, 17.05.2012 года У., действуя умышленно, из корыстных побуждений, желая наступления преступного результата, передал переносной ПОС-терминал модели VeriFone VX 510 М. для осуществления последним под видом оплаты туров платежных операций по зачислению на расчетный счет У. чужих денежных средств с расчетных счетов банковских карт.

Действуя в соответствии с разработанным планом и согласно отведенной ему функции, и в совершении преступления, 21.05.2012 года в 11 часов 12 минут, С. находясь в своей квартире, действуя из корыстных побуждений, в целях последующего совершения тайного хищения чужих денежных средств, группой лиц по предварительному сговору совместно с М. и У., используя данные магнитных полос чужой расчетной банковской карты, платежной системы «MasterCard», принадлежащей Arab Financial Services Company B.S.C. государства Бахрейн, полученные им в результате собирания незаконным способом сведений, составляющих банковскую тайну и записанные на заранее приготовленную пластиковую карту при помощи принадлежащего ему энкодера «MSR206u» и компьютерной программы «MSR206 Demo AP (206DDX51)», установленной на жестком диске принадлежащего ему ноутбука «Samsung», MODEL CODE: NP-R425-JS02RU, заведомо предназначенной для несанкционированного копирования компьютерной информации, провел последнюю через ПОС-терминал оплаты модели VeriFone VX 510 под видом осуществления операции по оплате тура, не имея на то законных оснований, то есть противоправно и втайне от сотрудников банка, не осведомленных о преступных намерениях участников сговора, направил в указанный банк запрос на перевод чужих денежных средств в сумме 127 260 руб., на расчетный счет, принадлежащий У., открытый последним в банке.

Однако данная операция была приостановлена, а денежные средства в общей сумме 127 260 руб. заблокированы руководителем группы мониторинга и подозрительных операций Департамента Безопасности и защиты информации Центрального офиса банка и не были зачислены на расчетный счет, принадлежащий индивидуальному предпринимателю У., в связи с чем, преступление не было доведено до конца по независящим от участников преступления обстоятельствам. Исходя из первоначальной позиции следствия, своими действиями участники преступления причинили банку вред деловой репутации.

Однако постановлением Советского районного суда г. Краснодара от 20.09.2012 года (оставленным без изменения определением суда кассационной инстанции) данное уголовное дело было возвращено прокурору Краснодарского края в порядке ст. 237 УПК РФ для устранения допущенных нарушений норм УПК РФ. В обоснование принятого постановления судом первой инстанции было указано, что органами предварительного следствия по вмененному обвинению всем подсудимым материальному составу преступления, к которому

относится ст. 158 УК РФ, в данном случае вмененная через ч. 3 ст. 30 УК РФ как покушение на тайное хищение чужого имущества, не установлено и не указано, конкретно чьи денежные средства пытались похитить подсудимые. В данном случае, это могло быть лицо с чьего персонального счета были бы сняты денежные средства, либо в результате данных действий пострадал бы в материальном плане непосредственно банк, которому как указано в обвинительном заключении был причинен вред деловой репутации, чего в данном случае недостаточно и причинение такого рода вреда не образует состава преступления, предусмотренного ст. 158 УК РФ.

Однако в данном случае нельзя не отметить некоторую двойственность в подходе к понятию собственника денежных средств на банковском счете. Так, согласно Постановлению арбитражного суда кассационной инстанции – Федерального арбитражного суда Волго-Вятского автономного округа от 29 октября 2002 года Дело № А43-1208/01-15-44-12исп следует, что по смыслу статей 845 и 854 Гражданского кодекса Российской Федерации, а также пункта 1.16 Правил ведения бухгалтерской отчетности в кредитных организациях, расположенных на территории Российской Федерации, утвержденных приказом Центрального банка Российской Федерации от 18.06.1997 № 02-263, следует, что денежные средства, находящиеся на банковском счете (расчетном (текущем), открытом банком клиенту (владельцу счета), являются собственностью владельца счета, а операции по нему осуществляются по распоряжению клиента о перечислении и выдаче соответствующих сумм со счета и проведении других операций. То есть собственником денежных средств на банковской карте является то лицо, на которое открыт данный банковский счет, но отнюдь не банк. Косвенно данный факт также подтверждается Постановлением кассационной инстанции по проверке законности и обоснованности решений (постановлений) арбитражных судов, вступивших в законную силу – ФАС ВСО от 21 сентября 2006 г. Дело № А19-31544/04-33-Ф02-4854/06-С1, в мотивировочной части решения которого суд кассационной инстанции указывает, что в соответствии с пунктом 2 статьи 209 Гражданского кодекса Российской Федерации собственник вправе по своему усмотрению совершать в отношении принадлежащего ему имущества любые действия, не противоречащие закону и иным правовым актам и не нарушающие права и охраняемые законом интересы других лиц, в том числе отчуждать свое имущество в собственность другим лицам, передавать им, оставаясь собственником, права владения, пользования и распоряжения имуществом, отдавать имущество в залог и обременять его другими способами, распоряжаться им иным образом. На основании пункта 3 статьи 845 Гражданского кодекса Российской Федерации банк не вправе определять и контролировать направления использования денежных средств клиента и устанавливать другие, не предусмотренные законом или договором банковского счета ограничения его права распоряжаться денежными средствами по своему усмотрению.

Следовательно, банки не наделены правом осуществлять контроль за целевым использованием находящихся на расчетном счете их клиентов денежных средств. Изменять назначение платежа вправе только собственник перечисляемых денежных средств.

По мнению же Н. Потапенко, для того, чтобы определить происшедшее как хищение, необходимо, чтобы деяние содержало все его признаки. В примечании к ст. 158 УК определено, что «под хищением... понимаются совершенные с корыстной целью противоправные безвозмездные изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества». Попытаемся теперь выяснить, охватывается ли данным определением незаконное использование банковской карты. В качестве предмета хищения в данном случае выступают наличные деньги, полученные из банкомата, либо приобретенный в магазине товар. При «обналичивании» карты после ввода PIN-кода и авторизации лицо, использующее эту карту, может распорядиться находящимися на счете денежными средствами, получая их наличными. В большинстве случаев так и происходит: преступник вводит значение суммы к снятию со счета, и банкомат выдает ему деньги. В данном случае одновременно происходит изъятие денег из чужого законного владения (банка – собственника выдаваемых наличных денег) и обращение их злоумышленником в свою пользу. При этом такие изъятие и обращение осуществляются безвозмездно, с корыстной целью и причиняют ущерб собственнику имущества [7]. Кроме того, теоретически в данном случае возможны три варианта лиц, которых следует признать потерпевшим: банк-эквайрер, банк-эмитент карты, законный держатель карты – владелец банковского счета. Наличие таких вариантов обусловлено пробелами в регулировании системы безналичных расчетов.

Как следует из положений п.2 Постановления Пленума Верховного Суда РФ от 29 июня 2010 г. № 17 «О практике применения судами норм, регламентирующих участие потерпевшего в уголовном судопроизводстве», в соответствии с законом потерпевший, являясь физическим лицом, которому преступлением причинен физический, имущественный или моральный вред, либо юридическим лицом в случае причинения преступлением вреда его имуществу и деловой репутации, имеет в уголовном процессе свои собственные интересы, для защиты которых он в качестве участника уголовного судопроизводства со стороны обвинения наделен правами стороны. Лицо, пострадавшее от преступления, признается потерпевшим независимо от его гражданства, возраста, физического или психического состояния и иных данных о его личности, а также независимо от того, установлены ли все лица, причастные к совершению преступления. Если совершенное преступление являлось неоконченным (приготовление к тяжкому или особо тяжкому преступлению или покушение на преступление), суду при решении вопроса о признании лица потерпевшим следует установить, в чем выразился причиненный ему вред. При этом не исключается возможность

причинения такому лицу морального вреда в случаях, когда неоконченное преступление было направлено против конкретного лица.

При таких обстоятельствах, по нашему мнению, необходимо включить в вышеуказанное постановление Пленума Верховного Суда РФ дополнение о том, что в случае, если совершено тайное хищение (либо покушение на тайное хищение) денежных средств, находящихся на банковском счете (в связи с использованием банковской карты), то необходимо признавать потерпевшими и лицо – собственника денежных средств, на чье имя открыт данный вклад и банк, деловой репутации которого как владельца денежных средств причинен вред. Только в этом случае будут соблюдены требования ч. 1 ст. 2 УК РФ.

Кроме того, по нашему мнению, по вышеуказанными причинам, следует внести изменения в УК РФ, дополнив ее статьей «компьютерное хищение» с целью избегания ошибок и неясностей в квалификации совершенных киберпреступлений.

Список литературы

1. Богданов В. Пластиковая отмычка. http://www.rg.ru/2006/02/10/plastik.html. Дата обращения: 23.08.2014 г.
2. Бражник С.Д. Проблемы совершенствования норм об ответственности за преступления, связанные с компьютерной техникой // Налоговые и иные экономические преступления: Сб. науч. ст. Вып. 2. – Ярославль, 2000. – С. 80.
3. Воронцова С.В. Киберпреступность: проблемы квалификации преступных деяний // СПС «Консультант плюс. – 2014.
4. Журавлев М., Журавлева Е. Актуальные вопросы судебной практики по уголовным делам о мошенничестве // Уголовное право. – 2008. – № 3. – С.17.
5. Завидов Б.Д. Комментарий действующего законодательства о защите объектов интеллектуальной собственности и сферы высоких технологий // Библиотечка Российской газеты. – 2003. – № 16. – С. 139-140.
6. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет: автореф. дис. … канд. юрид. наук. – Саратов, 2011. – С. 16.
7. Потапенко Н. О проблемах уголовной ответственности за преступления с использованием банковских карт // Уголовное право. – 2007. – № 4. – С. 27.
8. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно – правовая и криминологические характеристики: дис. … канд. юрид. наук. Иркутск, 2006. – С. 109-112.
9. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук. – Владивосток, 2005. – С. 112.

10. Хилюта В.В. Уголовная ответственность за хищения с использованием компьютерной техники // Журнал Российского права. – 2014. – № 1. – С. 29.
11. Чекунов И.Г. Криминологические и уголовно-правовые аспекты предупреждения киберпреступлений // Российский следователь. – 2013. – № 3. – С. 41.
12. Kaspersky Security Network http://www.kaspersky.ru/ downloads/pdf/ kaspersky_ security_network.pdf. (Дата обращения: 23.08.2014).

Рецензенты:

Костенко Н.И., д.ю.н., профессор, начальник юридического отдела ООО НПО «Нива», ст. Ленинградская.

Косарев С.Ю., д.ю.н., профессор, профессор кафедры уголовно- правовых дисциплин Санкт-Петербургской юридической академии, г. Санкт-Петербург.