НЕКОТОРЫЕ ОСОБЕННОСТИ БОРЬБЫ С ТРАНСНАЦИОНАЛЬНЫМ КОМПЬЮТЕРНЫМ МОШЕННИЧЕСТВОМ

Филимонов С.А.

кандидат юридических наук, соискатель ученой степени доктора юридических наук, руководитель базового адвокатского образования Ленинградского района Краснодарского края, 353740, Краснодарский край, Ленинградский район, станица Ленинградская, ул. Чернышевского, д. 199, к.12, filinlow@rambler.ru

УДК 351.74 (470)
ББК 67.7 (2Рос)

Цель. Изучение причин низких результатов в борьбе с компьютерным мошенничеством.

Методы. Методологическую основу данной работы составляет диалектический метод познания с применением принципов развития, целостности и системности. В работе применялись общенаучные и специальные юридические методы: сравнительный, системно-структурный, теоретико-методологический и др. Изучены изменения в действующем международном законодательстве по борьбе с компьютерным мошенничеством, обобщены практические результаты, имеющиеся в этом направлении борьбы с преступностью со стороны Европейского центра по борьбе с киберпреступностью (ЕС-3), а также проанализирована имеющаяся практика следственных и судебных органов Российской Федерации по борьбе с киберпреступностью.

Результаты. Исходя из изучения динамики резкого увеличения количества киберпреступлений и прежде всего компьютерного мошенничества автор приходит к выводам о необходимости срочного усиления борьбы с компьютерным мошенничеством посредством объединения усилий правоохранительных органов всех государств мира, обязательной криминализации киберпреступлений во всех государствах, координации слаженной работы всех правоохранительных органов России, в компетенцию которых входит борьба с компьютерным мошенничеством. Автором делается мотивированный вывод о необходимости срочного усиления санкции за совершение компьютерного мошенничества, вносятся предложения по координации борьбы с компьютерным мошенничеством со стороны всех институтов гражданского общества России.

Научная новизна. В порядке констатации следует заявить о том, что вплоть до настоящего времени в российской науке уголовного права недостаточно предпринимались исследования по указанной проблеме. Научная новизна заключается в конструктивном исследовании действующих международных конвенций по борьбе с компьютерным мошенничеством, выявлении явных противоречий в данных нормативных актах, детальном изучении практики борьбы правоохранительных органов РФ с компьютерным мошенничеством.

Ключевые слова: транснациональные преступления, киберпреступления, уголовное право, Европол, компьютерное мошенничество.

CERTAIN SPECIFICS OF COMBATING TRANSNATIONAL CYBERCRIME

Filimonov S.A.

Candidate of Legal Sciences, applicant for the degree of Doctor of Legal Sciences, Head of the fundamental legal education of Leningradsky rural district, Krasnodar region, fl.12, 199, Chernyshevsky str., Leningradskaya village, Leningradsky rural district, Krasnodar region, 353740, filinlow@rambler.ru

Purpose. The study of the causes of poor results in fighting cybercrime.

Methods. The methodological basis of this work is the dialectical method of cognition with application of the development, holistic and systemic principles. The paper used scientific and special legal methods: comparative, systemic and structural, theoretical and methodological and others. Changes in the international legislation to combat cybercrime are studied, practical results available in this field of combating crime on the part of the European Centre for Combating cybercrime (EU-3) are summarized and the existing practice of investigative and judicial authorities of the Russian Federation in the fight against cybercrime is analyzed.

Results. Based on researching the dynamics of a sharp increase in the number of cybercrimes and computer fraud in particular the author draws the conclusions of the urgency to strengthen the fight against computer fraud by combining the efforts of law enforcement agencies of all countries in the world, of the mandatory criminalization of cybercrime in all states, of coordinated teamwork of all law enforcement agencies of Russia responsible to fight against computer fraud. The author draws a reasonable conclusion about the urgent need to strengthen the penalties for committing cybercrime, and makes proposals to coordinate the fight against cybercrime by all the institutions of civil society in Russia.

Scientific novelty. It should be stated that up to the present time this problem hasn't been researched enough in the Russian science of criminal law. Scientific novelty lies in the constructive study of the existing international conventions against computer fraud, in identifying direct contradictions in these regulations, in studying carefully the practice of the Russian Federation law enforcement agencies to combat cybercrime.

Key words: transnational crime, cybercrime, criminal law, Europol, computer fraud.

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.

Одними из наиболее опасных транснациональных преступлений, на наш взгляд, являются киберпреступления. Как следует из п.2 Конвенции ООН «Против транснациональной организованной преступности» от 15 ноября 2000 года (ратифицирована РФ Федеральным законом от 26.04.2004 № 26-ФЗ и вступила в силу на территории России с 25 июня 2004 года), преступление носит транснациональный характер, если:

a) оно совершено в более чем одном государстве;

b) оно совершено в одном государстве, но существенная часть его подготовки, планирования, руководства или контроля имеет место в другом государстве;

c) оно совершено в одном государстве, но при участии организованной преступной группы, которая осуществляет преступную деятельность в более чем одном государстве; или

d) оно совершено в одном государстве, но его существенные последствия имеют место в другом государстве [1].

По данным отчета Европола «The EU Serious and Organized Crime Threat Assessment» (SOCTA) 2013» только на территории Европейского союза обезврежено 3600 преступных группировок, осуществляющих свою деятельность в сети Internet, целью которых была личная финансовая выгода и подрыв экономической стабильности. Эксперты Европола вынуждены отметить, что в настоящее время выявляется порядка 30% всех киберпреступлений и прогнозируют в будущем увеличение числа совершаемых в этой сфере преступных деяний, связывая рост киберпреступности с увеличением значимости Интернета в повседневной жизни. Также данные эксперты отмечают, что увеличение значения мобильных устройств в качестве основного средства доступа к интернет – ресурсам может привести к более широкому использованию этих устройств преступниками [2].

С 11 января 2013 года в Гааге начал работу Европейский центр по борьбе с киберпреступностью (ЕС-3) в качестве структурного подразделения Европейской полицейской организации (Европола).

Данное подразделение Европола должно стать главным инструментом в борьбе с киберпреступностью на территории Европейского Союза. ЕС-3 займется созданием оперативных и аналитических мощностей, необходимых для обеспечения быстрого реагирования на киберпреступления, а также организацией взаимодействия официальных ведомств ЕС и стран-членов с международными партнерами.

Мандат деятельности Центра включает борьбу со следующими видами киберпреступности:

- преступления, совершенные организованными группами для получения незаконных доходов, такими как мошенничество с кредитными картами или банковскими операциями;

- преступления, нанесшие серьезный вред жертве, в частности с растлением и совращением малолетних;

- преступления, нанесшие вред критически важным инфраструктурным и информационным системам в ЕС.

Также Центр займется сбором и обработкой данных, оказанием информационной, технической и криминалистической поддержки соответствующим подразделениям правоохранительных органов стран-членов ЕС, координацией совместных расследований, обучением и подготовкой специалистов (в сотрудничестве с CEPOL). Центр будет содействовать проведению необходимых исследований и созданию программного обеспечения (R&D), заниматься оценкой и

анализом существующих и потенциальных угроз, составлением прогнозов и выпуском заблаговременных предупреждений. В сферу деятельности Центра также будет входить помощь судьям и прокурорам. По оценкам представителей Европола, ежегодный ущерб от киберпреступности в мире оценивается в 290 млрд. евро. Лишь за прошлый год из-за действий киберпреступников граждане ЕС понесли прямой ущерб на 1,5 млрд. евро. Это делает киберпреступность более выгодной, чем торговля марихуаной, кокаином и героином вместе взятыми [3].

Как обоснованно указывала Н. Кроес, Европейский комиссар по вопросам внедрения новых технологий, в своем выступлении на Всемирном экономическом форуме в Давосе в 2013 г., самой серьезной ошибкой является неверное толкование обеспечения кибербезопасности как исключительно технического задания, поскольку главным субъектом ее обеспечения должно быть государство. Стратегической задачей является повышение эффективности кибербезопасности на всех уровнях государственной власти [4].

Согласно Конвенции «О преступности в сфере компьютерной информации», заключенной в г. Будапеште в 2001 году и вступившей в силу с 01 июля 2004 года киберпреступлениями являются деяния, направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей и компьютерных данных, а также злоупотребления такими системами, сетями и данными [5]. Согласно ст. 12 данной Конвенции предусмотрено введение уголовной ответственности юридических лиц, что противоречит действующему российскому уголовному законодательству. Как обоснованно указывают С.С. Арбузов и С.П. Кубанцев, на настоящий момент существующие положения по введению уголовной ответственности юридических лиц в России носят поверхностный характер, игнорируют существующую доктрину уголовного права и в случае их реализации способны дезорганизовать систему уголовного судопроизводства и стать дополнительным источником коррумпированности правоохранительных и иных государственных органов [6, с.106].

В связи с острой необходимостью борьбы с киберпреступностью 01 июня 2001 года в г. Минске было заключено Соглашение о сотрудничестве государств - участников содружества независимых государств в борьбе с преступлениями в сфере компьютерной информации (ратифицировано РФ с оговоркой Федеральным законом от 01.10.2008 № 164-ФЗ и вступило в силу на территории России с 17.10.2008 года) [7].

Как следует из ст. 1 вышеуказанного Соглашения преступление в сфере компьютерной информации - уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация.

С учетом того факта, что вышеуказанные международные правовые акты по борьбе с киберпреступностью обладают явной противоречивостью в том числе в самом понятии киберпреступления это может привести к уводу от уголовной ответственности преступника только потому, что государство, в котором было совершено киберпреступление и государство, в котором было задержано виновное лицо ориентируются на разные международные договора о борьбе с кибепреступлениями. Необходимо также отметить, что не все страны мира криминализировали киберпреступления. То есть совершение киберпреступлений в некоторых странах вообще уголовно не наказуемо, что приводит к появлению безнаказанных профессиональных интернет – преступников.

Для совершения киберпреступлений достаточно лишь приобрести портативное средство спутниковой связи. Время, в течение которого совершается этот вид преступлений, может занимать менее одной минуты и преступник не ограничен в выборе страны, на территории которой он это устройство будет использовать. У правоохранительных органов на поиск и привлечение к уголовной ответственности такого лица, как правило, уходит значительное количество времени, в течение которого преступник имеет реальную возможность уничтожить следы преступления, чем затруднить или сделать невозможным привлечение киберпреступника к уголовной ответственности. В данной ситуации только путем объединения усилий правоохранительных органов всех государств возможно эффективное пресечение этой категории транснациональных преступлений.

В связи с открытым доступом к сети Интернет большинство киберпреступлений совершается именно с использование данной сети, ведь отследить лицо, совершившее преступление весьма затруднительно. Одним из факторов, приводящих к росту данной категории преступлений в России, является отсутствие необходимого взаимодействия правоохранительных органов в вопросах расследования этих преступлений. В этой связи особое значение приобретает необходимость постоянного повышения профессиональной подготовки сотрудников правоохранительных органов по вопросам расследования данных преступлений.

Как обоснованно указывает П.В. Костин, преступления в сфере компьютерной информации редко встречаются в обособленном виде, как правило, они совершаются в совокупности с иными общественно опасными деяниями и имеют факультативный характер. Это обусловлено тем, что при использовании компьютерной информации в качестве средства совершения другого преступления она сама становится предметом общественно опасного деяния [8, с.6]. Значительные проблемы испытывают правоохранительные органы в борьбе с компьютерным мошенничеством. Так, на открытии IV международной конференции «Борьба с мо-

шенничеством в сфере высоких технологий. AntiFraud Russia – 2013» начальник БСТМ МВД России генерал – майор полиции Алексей Мошков отметил, что с каждым годом растет сложность мошеннических операций в Интернет, что предъявляет особые требования к квалификации сотрудников, занимающихся расследованием киберпреступлений. По итогам первых 9 месяцев 2013 года количество уголовных дел по линии Управления «К», направленных в судебные органы выросло на 12,6%.

БСТМ МВД России провело ряд успешных мероприятий по пресечению деятельности организованных преступных групп, занимающихся хищениями денежных средств с банковских счетов граждан и организаций. Кроме того, были установлены лица, причастные к созданию и использованию вредоносных программ, предназначенных для скрытого копирования реквизитов доступа к банковским счетам граждан и организаций. В общей сложности, сотрудники Управления «К» предотвратили хищения с банковских счетов граждан на сумму около 1 миллиарда рублей [9]. Необходимо отметить тот факт, что в течение длительного времени различными учеными предлагалось дополнить российское уголовное законодательство отдельной статьей, предусматривающей ответственность за компьютерное мошенничество. Так, по мнению Д. Айкова под компьютерным мошенничеством необходимо понимать корыстное преступное посягательство, в ходе выполнения которого осуществляются манипуляции с программами, данными или аппаратной частью ЭВМ [10, с.25]. Волеводз А.Г. предлагал ввести в УК РФ ст.159-1 «Компьютерное мошенничество», которое квалифицировать как завладение чужим имуществом путем обмана, злоупотреблением доверием, присвоения, растраты либо причинения имущественного ущерба путем обмана или злоупотребления доверием, совершенное с использованием ЭВМ, системы ЭВМ или их сети [11, с.75]. По мнению Черных А.В. компьютерное мошенничество – это умышленное искажение, изменение или раскрытие данных с целью получения выгоды с помощью компьютерной системы, которая используется для совершения или прикрытия одиночного или серийного преступления [12, с.71].

Согласно Федеральному закону № 207-ФЗ от 29.11.2012 года «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» УК РФ был дополнен статьей 159.6 «Мошенничество в сфере компьютерной информации», согласно которой под мошенничеством в сфере компьютерной информации понимается хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. При этом достаточно часто данное преступление совершается с использованием компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации из корыстной заинтересованности. В данной ситуации у органов предварительного следствия справедливо возникает вопрос о том, необходимо ли данные деяния квалифицировать по совокупности преступлений: ст.159.6 и ч.2 ст.273 УК РФ или только по статье «Мошенничество в сфере компьютерной информации». Представляется, что в этом случае необходимо квалифицировать деяния киберпреступников по совокупности вышеуказанных преступлений. Однако для правильного применения уголовного закона в этой ситуации необходимо разъяснение Верховного Суда РФ в ближайшем обзоре судебной практики.

Имеющиеся на данный момент судебные акты по ст.159.6 УК РФ свидетельствует о том, что некоторые государственные обвинители неправильно трактуют применение данной статьи УК РФ. Так, апелляционным определением Московского областного суда от 6 мая 2013 г. № 10-2076 оставлено без удовлетворения представление государственного обвинителя Якушиной Т.В. на приговор Люблинского районного суда г. Москвы от 19 февраля 2013 года, которым Д. признан виновным в совершении девяти мошенничеств в сфере компьютерной информации. 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 и действуя с учетом договоренности Д. изготавливал поддельные доверенности и получал дубликаты сим-карт и пароли.

Далее в период времени с 24.10.2011 года по 10.12.2011 года, Д., используя сим-карты и пароли через электронную систему "*-Онлайн" путем перечисления на счета и банковские карты различных лиц завладел денежными средствами - А. на общую сумму в 830.000 рублей; - М. на общую сумму в 258.000 рублей; - К. на общую сумму в 210.000 рублей; - П. на общую сумму 262.000 рублей; - Б. на общую сумму в 280.000 рублей; - С. на общую сумму в 300.000 рублей; - Р.; Н., М. на общую сумму в 600.000 рублей, каждому.

Несмотря на явно обоснованную квалификацию деяний осужденного по ст.159.6 УК РФ судом 1-й инстанции вышеуказанный государственный обвинитель в апелляционном представлении в частности указал, что для осуществления переводов денежных средств со счетов потерпевших Д. незаконно добился перевыпуска сим-карт потерпевших, используя которые путем введения достоверных логина и пароля осуществлял перечисление денежных средств потерпевших через систему "* Онлайн". Данная судом 1-й инстанции квалификация этих действий как мошенничество в сфере компьютерной информации, по мнению государственного обвинителя, несостоятельна, поскольку указанные действия образуют простое мошенничество [13]. По нашему мнению в приведенном случае налицо банальное незнание государственным обвинителем отличий объективной стороны составов преступлений, предусмотренных ст. ст. 159.6 и 159 УК РФ соответственно. В отличие от состава преступления, предусмотренного ст. 159 УК РФ мошенничество в сфере компьютерной информации совершается путем вмешательства в функционирование компьютера или компьютерной сети. Обман в этом случае может выражаться в искажении данных компьютерных систем, в манипуляции с данными о переходе имущества от одного лица к другому.

Не может не вызывать обеспокоенность тот факт, что санкция ст.159.6 УК РФ значительно ниже, чем санкция ст.159 УК РФ. Более того, за совершение неквалифицированного мошенничества в сфере компьютерной информации даже не предусмотрено наказание в виде лишения свободы. А ведь угроза киберпреступности настолько сильна, что в российской армии до конца 2013 года должен был появиться отдельный род войск, который будет заниматься борьбой с киберугрозами. Впервые о планах создания киберкомандования в марте 2013 года заявил заместитель председателя Правительства РФ Дмитрий Рогозин. Он заявил, что все необходимые для этого документы уже подготовлены и в российской армии создается род войск, в задачи которого будет входить обеспечение информационной безопасности страны. По словам военного эксперта Анатолия Цыганка: «Концепция применения кибероружия разработана шесть–семь лет назад. Сейчас это оружие является вторым по значимости после ядерного. Кибероружие активно применяется в военных конфликтах. Последний пример – в ходе интервенции США в Ливии, где они контролировали не только воздушное пространство (они нарушили всю систему ПВО), но и телекоммуникационные сети. Они входили в ливийские телесети и передавали передачи для местного населения».

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 денеж-

ные 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 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.

При этом постановлением Советского районного суда г. Краснодара от 20.09.2012 года (оставленным без изменения определением суда кассационной инстанции) данное уголовное дело было возращено 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 [14].

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 N 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 которо-

го 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 [15, с.27].

В свете данных событий необходимо не только незамедлительно значительно усилить санкцию за совершение компьютерного мошенничества, то есть наказывать за данное преступление в обязательном порядке в виде лишения свободы, но и подготовить эффективные меры стимулирования частно - государственного партнерства в области дополнительного профессионального образования по направлению кибербезопасности. Возникает срочная необходимость разработки и введения актуальных периодически обновляемых учебных курсов повышения квалификации в области противодействия компьютерному мошенничеству для преподавательских кадров и государственных служащих, вовлеченных в процессы обеспечения кибербезопасности государства, организаций и граждан.

Кроме того, в свете изложенных фактов необходимо дополнить УК РФ дополнительной статьей об уголовной ответственности за киберхалатность в отношении руководителей компаний интернет – провайдеров и сотовых операторов за бездействие, позволившее совершить киберпреступление. При этом также необходимо распределить и гражданско – правовую ответственность исходя из степени вины киберпреступника и интернет-провайдера (оператора сотовой связи).

Следует также отметить тот факт, что только в результате консолидации усилий правоохранительных органов и всех институтов гражданского общества возможно добиться реальных успехов в борьбе с компьютерным мошенничеством.

Литература:

1. Конвенция против транснациональной организованной преступности от 15 ноября 2000 г. (г. Нью-Йорк). Принята Резолюцией 55/25 на 62-ом пленарном заседании 55-ой сессии Генеральной Ассамблеи ООН // Собрание законодательства РФ. 2004. № 40. Ст. 3882.
2. Отчет Европола «The EU Serious and Organized Crime Threat Assessment (SOCTA) 2013» [электронный ресурс]. URL: ttps://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf (дата обращения 25.03.2014).
3. European Institute for Crime Prevention and Control, affiliated with the United Nations (NEUNI) [электронный ресурс] // Retrieved on December 15 2006. URL: http://www.ulapland.fi/home/oiffi/enlist/resources/Heuniweb/htm (дата обращения 25.03.2014).
4. Kroes Neelie. Speech: EU Cybersecurity Strategy [электронный ресурс]. URL: http://europa.eu/rapid/press-release_SPEECH-13-51_en.htm. http://www.ulapland.fi/home/oiffi/enlist/resources/Heuniweb/htm (дата обращения 25.03.2014.).
5. Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 (г. Будапешт) [электронный ресурс]. URL: http://www.lawmix.ru/abro/3454 (дата обращения 25.03.2014.).
6. Арбузов С.С., Кубанцев С.П. О перспективе введе-

ния в России института уголовной ответственности юридических лиц // Журнал российского права. 2012. № 10.
7. Соглашение о сотрудничестве государств - участников содружества независимых государств в борьбе с преступлениями в сфере компьютерной информации [электронный ресурс]. URL: http://www.bestpravo.ru/rossijskoje/er-postanovlenija/v3w.htm (дата обращения 25.03.2014.).
8. Костин П.В. Исследование машинных носителей информации, используемых при совершении преступлений в сфере экономики: Автореф. дис. ... к.ю.н. Н. Новгород, 2007.
9. Международная конференция AntiFraud Russia – 2013 успешно завершила свою работу [электронный ресурс]. URL: http://club.cnews.ru/blogs/entry/mezhdunarodnaya_ konferentsiya antifraud_russia_ (дата обращения 25.03.2014.).
10. Айков Д. Компьютерные преступления. М., 1999.
11. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., 2002.
12. Черных А.В. Некоторые вопросы уголовно – правовой квалификации компьютерных мошенничеств // Советское государство и право. 1989. № 6.
13. Архив Московского областного суда. Уголовное дело № 10-2076.
14. Архив Советского районного суда г. Краснодара. Уголовное дело № 390430.
15. Потапенко Н. О проблемах уголовной ответственности за преступления с использованием банковских карт. Уголовное право. 2007. №4.

References:

1. Convention against Transnational Organized Crime of 15 November 2000 (New York City). Approved by Resolution 55/25 at the 62nd plenary meeting of the 55th session of the UN General Assembly // Collected Legislation of the Russian Federation. 2004. № 40. Art. 3882.
2. Europol Report “The EU Serious and Organized Crime Threat Assessment (SOCTA) 2013" [e-resource]. URL: ttps://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf (date of access 25.03.2014).
3. European Institute for Crime Prevention and Control, affiliated with the United Nations (NEUNI) [e-resource] // Retrieved on December 15 2006. URL: http://www.ulapland.fi/home/oiffi/enlist/resources/Heuniweb/htm (date of access 25.03.2014).
4. Kroes Neelie. Speech: EU Cybersecurity Strategy [e-resource]. URL: http://europa.eu/rapid/press-release_SPEECH-13-51_en.htm.http://www.ulapland.fi/home/oiffi/enlist/resources/Heuniweb/htm (date of access 25.03.2014.).
5. Convention on crime in the field of computer information on 23 November 2001 (Budapest) [e-resource]. URL: http://www.lawmix.ru/abro/3454 (date of access 25.03.2014.).
6. Arbuzov S.S., Kubantsev S.P. On the perspectives of introducing in Russian of the institute of criminal liability of legal entities // Journal of Russian law. 2012. № 10.
7. Cooperation Agreement of states - members of the Commonwealth of Independent States in the fight against crime in the sphere of computer information [e-resource]. URL: http://www.bestpravo.ru/rossijskoje/er-postanovlenija/v3w.htm (date of access 25.03.2014.).
8. Kostin P.V. The study of computer media used in committing crimes in the sphere of economy: Abstr. Dis. ... Cand Law. Nizhny Novgorod, 2007.
9. International Conference AntiFraud Russia - 2013 has successfully completed its work [e-resource]. URL: http://club.cnews.ru/blogs/entry/mezhdunarodnaya_ konferentsiya antifraud_russia_ (date of access 25.03.2014.).
10. Ayikov D. Computer crimes. M., 1999.
11. Volevodz A.G. Combating computer crime: legal-framework for international cooperation. M., 2002.
12. Chernykh A.V. Some issues of criminal - legal qualification of computer fraud // Soviet state and law. 1989. № 6.
13. Archive of the Moscow Regional Court. The criminal case № 10-2076.
14. Archives of the Soviet District Court of Krasnodar. Criminal case № 390430.
15. Potapenko N. On the problems of criminal responsibility for crimes involving bank cards. Criminal law. 2007. №4.