УДК 343.2

УГОЛОВНАЯ ПОЛИТИКА РОССИИ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ: СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ

О.Ю. Савельева, кандидат юридических наук, доцент, доцент кафедры «Уголовное право и процесс»
К.А. Забурдаева, преподаватель кафедры «Уголовное право и процесс»
Д.Н. Мединовская, магистрант кафедры «Уголовное право и процесс»
Тольяттинский государственный университет, Тольятти (Россия)

Ключевые слова: киберпреступления; информационная безопасность; мошенничество в сфере компьютерной информации; компьютерное мошенничество; компьютерная информация; электронные средства платежа.

Аннотация: Активный и непрерывный процесс информационного развития, сопровождающийся появлением новых цифровых инфраструктур, технологий вычислительной техники и цифровых коммуникаций, с одной стороны, положительным образом сказывается на всех сферах человеческой жизнедеятельности, способствуя улучшению качества жизни. Но, с другой стороны, данные процессы, несут и негативные последствия. За последние годы значительно увеличилось число хищений, совершаемых не традиционным способом, а с помощью различных продуктов технологического и информационного прогресса (к примеру, в сети Интернет). Таким образом, правоохранительные органы всего мира столкнулись с новым негативным социальным явлением – киберпреступлением.

Проведен сравнительно-правовой анализ российского и белорусского законодательства, а также материалов судебной практики двух стран. При этом особо пристальное внимание обращено на исследование мошенничества в сфере компьютерной информации. Проанализированы точки зрения ряда российских и белорусских ученых, касающиеся понимания термина «киберпреступность». Проведен анализ статистических данных о состоянии киберпреступности за период 2016–2018гг. и произведена оценка этих данных. Полученные данные позволяют сделать вывод об отрицательной криминологической динамике киберпреступлений как в России, так и на территории Белоруссии, об интенсивном росте некоторых видов киберпреступлений (мошенничество в сфере компьютерной информации и мошенничество, совершаемое с использованием электронных средств платежа; иные преступления, совершаемые посредством сети Интернет), а также о несовершенстве уголовной политики в части противодействия данному виду преступлений. Предлагается пересмотреть положения уголовного законодательства в части регламентации ответственности за отдельные виды киберпреступлений, а также уточнить позицию Верховного Суда РФ по вопросам отнесения к определенному виду хищения деяний, совершаемых в киберпространстве.

ВВЕДЕНИЕ

По сведениям Генпрокуратуры РФ, «число преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, с 2013 г. по 2016 г. увеличилось в 6 раз – с 11 тыс. до 66 тыс.» [1]. За 2017 г. было зарегистрировано 90 587 таких преступлений, что составляет более 13 тыс. в месяц (в 2016 г. в среднем было совершено 7,5 тыс. преступлений в месяц). В 2018 г. опять же отмечался рост киберпреступлений. Их число составило 174 674. При этом только с 2015 г. по 2016 г. в шесть раз выросло число мошенничеств (с 2,2 тыс. до 13,4 тыс.) и более чем в три раза выросло число краж, совершаемых с помощью Интернета и иных коммуникационных ресурсов (с 2,3 тыс. до 8,5 тыс.). В 5,5 раза (с 995 до 5,5 тыс.) выросло количество преступлений, связанных с хищением, удалением, блокировкой компьютерной информации с целью мошенничества (ст. 159.6 УК РФ) [2].

Однако проблема киберпреступности актуальна не только для российского общества. Так, по данным статистики МВД республики Беларусь, по сравнению с 2017 г. в 2018 г. на территории государства увеличилось на 53,0 % (с 3 099 до 4 741) количество зарегистрированных киберпреступлений. Более двух третьих преступлений в сфере высоких технологий (75,6 % или 3 585; 2017 г. – 74,8 % или 2 318) относятся к хищениям, совершаемым с использованием компьютерной техники (ст. 212 УК). Число особо тяжких и тяжких преступлений увеличилось на 2,3 % (с 43 до 44). Количество выявленных преступлений против информационной безопасности (ст.ст. 349–355 УК) увеличилось в целом по республике на 48,0 % (с 781 до 1 156). При этом констатируется факт, что рост числа уголовно наказуемых деяний против информационной безопасности обусловлен увеличением количества преступлений, связанных с несанкционированным доступом к компьютерной информации (+97,4 %; с 462 до 912) [3].

Такая отрицательная криминологическая динамика не могла не отразиться на уголовной политике как России, так и Белоруссии. Так, российским законодательством был принят ряд уголовно-правовых мер, направленных на реформирование ответственности за мошенничество. К примеру, Федеральным законом от 29.11.2012 г. №207-ФЗ в Уголовный кодекс РФ (далее – УК РФ) были включены шесть специальных видов мошенничества. Два из них касаются киберпреступности – мошенничество в сфере компьютерной информации (ст. 159.6) и мошенничество, совершаемое с помощью платежных карт (ст. 159.3). Федеральным законом от 23.04 .2018 г. №111-ФЗ последняя норма подверглась изменениям: теперь в ней говорится о мошенничестве, совершаемом с помощью электронных средств платежа.

Верховным Судом Российской Федерации были даны рекомендации по особенностям применения указанных норм о мошенничестве в Постановлении Пленума Верховного Суда РФ от 30.11.2017 г. №48 «О судебной практике по делам о мошенничестве, присвоении и растрате» (далее – Постановление Пленума ВС РФ от 30.11.2017 г. №48) и в Постановлении Пленума Верховного Суда РФ от 15.11 2016 г. №48 «О практике применения судами законодательства, регламентирующего особенности уголовной

ответственности за преступления в сфере предпринимательской и иной экономической деятельности».

Законодатель республики Беларусь пошел по аналогичному пути, однако принятых «специальных» норм о мошенничестве в Уголовном кодексе Республики Беларусь (далее – УК РБ) намного меньше, чем в УК РФ, и они охватываются диспозицией одной статьи, а именно статьей 212 (хищение, совершаемое с использованием компьютерной техники).

Вопросу увеличения количества киберпреступлений посвящены работы многих ученых. Так, уже восемь лет назад И.Г. Чекунов обращал внимание на проблемы квалификации мошенничества, предметом которого являются «электронные деньги» [4]. В более поздних статьях уже фигурирует термин «киберпреступление». В частности, Э.Н. Харина проводит уголовно-правовой и криминалистический анализ данной категории преступлений, акцентируя, однако, внимание на изучении компьютерных преступлений [5], как и ряд других авторов [6–8]. Проблемы киберпреступлений в сфере отношений собственности рассматриваются в трудах ученых [9–11]. Однако все исследования в данной сфере, как правило, имеют предположительный характер, их нельзя считать завершенными. В силу чрезмерно высокой интенсивности развития киберпреступности уголовное законодательство и судебная практика требуют постоянного переосмысления и переработки.

Цель исследования – рассмотрение спорных вопросов законодательной регламентации ответственности за киберпреступления, проблем толкования киберпреступлений в научной доктрине и судебной практике и разработка предложений, направленных на повышение эффективности борьбы с киберпреступлениями.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Анализ содержания диспозиций статей 159.6 УК РФ и 212 УК РБ позволяет сделать определенные выводы, свидетельствующие о сходстве и различии российского и белорусского законодательства в части понимания мошенничества в сфере компьютерной информации:

Диспозиции ст. 159.6 УК РФ и ст. 212 УК РБ обладают бланкетным характером, то есть при выявлении признаков составов преступлений, закрепленных в указанных нормах, необходимо будет знать определенные нормативные предписания законодательных актов, например: Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; четвертой части ГК РФ; Федерального закона от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне» (российское законодательство); Закона республики Беларусь от 10.11.2008 г. №455-З «Об информации, информатизации и защите информации» (белорусское законодательство).

Основным непосредственным объектом рассматриваемых составов преступлений выступают общественные отношения, имеющие связь с отношениями собственности, вне зависимости от ее формы, дополнительным же объектом являются правоотношения, которые обеспечивают информационную безопасность, ввиду этого, рассматриваемое преступление является двухобъектным [4].

Предметом анализируемых и рассматриваемых видов мошенничеств будет выступать чужое имущество, а также право на чужое имущество и дополнительно компьютерная информация, с помощью которой виновный совершает обманные действия и овладевает чужим имуществом или приобретает право на имущество.

По конструкции объективной стороны оба состава преступлений являются материальными, так как считаются оконченными в момент наступления общественно опасных последствий в виде имущественного ущерба. А вот способы совершения преступлений различны. Так, способами совершения преступления, предусмотренного ст. 159.6 УК РФ, будут выступать: ввод компьютерной информации; удаление компьютерной информации; блокирование компьютерной информации; модификация компьютерной информации; вмешательство в функционирование средств хранения, обработки, передачи компьютерной информации [5].

Способ совершения преступления, предусмотренного ст. 212 УК РБ, иной, а именно: изменение информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных; введение в компьютерную систему ложной информации [8]. Полагаем, что норма, закрепленная в ст. 212 УК РБ, является более архаичной по сравнению с нормой, закрепленной в ст. 159.6 УК РФ, ввиду того, что она менее всего описывает, какие именно способы совершения данного рода преступления возможны, а ведь именно это фундаментально значимо для квалификации преступления.

Что касается санкций статей 159.6 УК РФ и 212 УК РБ, то здесь необходимо отметить, что ни одна из четырех частей ст. 159.6 УК РФ не предусматривает наказание в виде лишения права занимать определенные должности и заниматься определенной деятельностью, в отличие от ст. 212 УК РБ. Так, санкция ч. 1 ст. 212 УК РБ закрепляет лишение права занимать определенные должности и заниматься определенной деятельностью в качестве основного вида наказания. В ч. ч. 2–4 ст. 212 УК РБ лишение права занимать определенные должности и заниматься определенной деятельностью указано в качестве дополнительного наказания к лишению свободы. Такая позиция белорусского законодательства представляется более правильной и должна быть воспринята российским законодательством. Поэтому считаем целесообразным в основном составе ст. 159.6 УК РФ закрепить лишение права занимать определенную должность или заниматься определенной деятельностью в качестве основного наказания.

Мнения ученых по вопросам правовой природы компьютерного мошенничества не однообразны. Некоторые авторы, признавая электронную среду лишь средством совершения мошенничества, полагают, что компьютерное мошенничество не должно быть вынесено в отдельный состав [7; 12; 13]. Другие, наоборот, обосновывая особенности компьютерного мошенничества, говорят о специальном составе преступления [6; 10]. Так, С.В. Смолин настаивает на исключении ст. 159.6 УК РФ из уголовного закона. Автор мотивирует это тем, что нарушение законодательной техники и лишняя казуистичность правовой нормы не благоволит единообразному применению уголовного закона, что вводит в заблуждение правоприменителя, и рано или поздно будет приводить к следственным и судебным ошибкам, что в конечном итоге ведет к нарушению

принципа справедливости и уменьшению интенсивности уголовно-правовой охраны соответствующих общественных отношений [11]. В.М. Елин, наоборот, говорит о важности криминализации компьютерного мошенничества. Автор считает, что с включением ст. 159.6 в российское уголовное законодательство разрешается вопрос об участии Российской Федерации в мировых интеграционных процессах в сфере борьбы с киберпреступностью, вектор которых определяется положениями Конвенции. Закрепление статьи в УК РФ, по мнению автора, будет важным элементом для дифференциации уголовной ответственности [10].

Любопытных, по нашему мнению, взглядов придерживается В.Г. Шумихин, считающий, что мошенничество в сфере компьютерной информации представляет собой самостоятельную (седьмую) форму хищения чужого имущества, поскольку объективная сторона преступлений, предусмотренных ст. 159 и ст. 159.6 УК РФ, по основным конструктивным признакам не совпадает. Данные нормы не находятся в соотношении общей и специальной. В объективной стороне компьютерного мошенничества законодатель выделил иные способы совершения хищения, что не предполагает личностного контакта субъекта и потерпевшей стороны, а связано исключительно с манипуляциями, которые осуществляет субъект посредством технических средств [14]. Позицию данного автора разделяют и другие ученые [15]. По мнению ряда авторов, хищение имущества в виде денежных средств, находящихся на счете, путем «взлома» защиты охраняемой компьютерной информации следует квалифицировать как кражу, поскольку компьютер – не физическое лицо, а фактически устройство, как и банкомат [16; 17].

Приведем краткий пример судебной практики, который иллюстрирует неоднозначность квалификации хищения, совершаемого с использованием компьютерных технологий:

Приговором Мирового судьи Судебного участка 134 Юрлинского муниципального района № 1-2 от 01.02.2018 г. Н. была признана виновной по ч. 1 ст. 158 УК РФ за совершение кражи при следующих обстоятельствах: около 16 часов Н., находясь у себя дома, употребила спиртные напитки совместно с Ф. Затем Ф. попросил Н. перевести с лицевого счета его мобильного банка на счет Н. 200 рублей для дальнейшего приобретения спиртного. Н. обнаружила, что баланс денежных средств на счету Ф. составил 5 000 рублей. Тогда у неё возник умысел на хищение денежных средств, принадлежащих Ф. Для реализации задуманного Н. тайно, из корыстных побуждений, осуществила перевод с лицевого счета Ф. на свой лицевой счет денежные средства в сумме 5 000 руб. После этого Н. денежные средства обналичила. Полученными денежными средствами в сумме 4 800 рублей Н. воспользовалась по своему усмотрению. На 200 рублей, по достигнутой изначально договоренности с Ф., приобрела бутылку водки. В результате своих действий Н. причинила Ф. материальный ущерб в размере 4 800 рублей. Судом Н. была признана виновной в совершении кражи по ч. 1 ст. 158 УК РФ [18].

Похожее уголовное дело было рассмотрено Дмитровградским городским судом. Однако действия обвиняемых Тямуковой А.Ф. и Панкратовой Л.Ж. были квалифицированы по ч. 2 ст. 159.6 УК РФ, то есть как мошенничество. Преступление было совершено при следующих обстоятельствах: 11.06.2017 г. в период времени с 01 часа до 02 часов 46 минут Тямукова А.Ф., находясь в помещении кафе «Ной», расположенном в доме 1 «б» по ул. Юнг Северного Флота г. Димитровграда Ульяновской области, предложила Панкратовой Л.Ж. совершить хищение денежных средств, принадлежащих Н., на что Панкратова согласилась. Осуществляя свой преступный умысел, Панкратова Л.Ж. взяла со стола оставленный Н. сотовый телефон «DEXP IXION ES135» с установленной внутри него сим-картой оператора сотовой связи «Т2 Мобайл», с подключенной к нему услугой ПАО «Сбербанк России» «Мобильный банк», выпущенной ПАО «Сбербанк России» на имя Н. Убедившись, что за их с Тямуковой А.Ф. преступными действиями никто не наблюдает, совместно обратились к К., не осведомленной о преступных намерениях Панкратовой Л.Ж. и Тямуковой А.Ф., с просьбой перевести с вышеуказанного расчетного счета потерпевшей Н. денежные средства на расчетный счет, зарегистрированный на К. После чего, согласившись с просьбой Панкратовой Л.Ж. и Тямуковой А.Ф., не осведомленная о преступных намерениях последних, К. назвала Панкратовой Л.Ж. и Тямуковой А.Ф. свой номер сотового телефона для перевода денежных средств на ее вышеуказанный расчетный счет. Тямукова А.Ф., во исполнение единого совместного преступного умысла, действуя по предварительному сговору с Панкратовой Л.Ж., находясь в вышеуказанном месте, в вышеуказанный период времени, взяв в руки вышеуказанный сотовый телефон, принадлежащий Н. с установленной внутри него сим-картой оператора сотовой связи «Т2 Мобайл» и подключенной к нему услугой ПАО «Сбербанк России» «Мобильный банк» для обслуживания вышеуказанного расчетного счета последней, отправила сообщение на номер 900 с содержанием «Перевод – (абонентский номер К.) 4 500», а Панкратова Л.Ж. в это время проверяла достоверность набранного Тямуковой А.Ф. абонентского номера К. В свою очередь К., не осведомленная о преступных намерениях Панкратовой Л.Ж. и Тямуковой А.Ф., в 02.56 часов того же дня, действуя по просьбе последних, используя личный сотовый телефон с установленным в нем Интернет-приложением «Сбербанк-Онлайн», осуществила перевод принадлежащих Н. денежных средств в сумме 4 500 рублей со своего расчетного счета на расчетный счет Тямуковой А.Ф., после чего последняя совместно с Панкратовой Л.Ж с места преступления скрылись, и в период времени с 02.56 до 03.30, находясь возле д. 16 по ул. Западная г. Димитровграда Ульяновской области, используя банкомат ПАО «Сбербанк России», незаконно сняли с расчетного счета Тямуковой А.Ф. 4 500 рублей, причинив Н. материальный ущерб на сумму 4 500 рублей [19].

А вот примеры из судебной практики республики Белоруссии, где содеянное было квалифицировано как мошенничество в сфере компьютерной информации по аналогии с вышеприведенным примером из практики Дмитровградского городского суда.

Так, 9.12.2014 г. Определением Судебной коллегии по уголовным делам Витебского областного суда оставлен без изменения приговор суда Железнодорожного района г. Витебска по уголовному делу по обвинению

гражданина Республики Беларусь в совершении преступлений, предусмотренных ч. 4 ст. 212, ч. 3 ст. 212, ст. 13 и ч. 2 ст. 212 и т. д. Как установлено судом, обвиняемый П. в период с 9.12.2012 г. до 30.04.2013 г., действуя по предварительному сговору с неустановленными лицами, используя заранее изготовленные поддельные платежные карточки, реквизиты которых были скопированы им же с магнитных полос карточек потерпевших при помощи скимминговых устройств, установленных на картоприемники банкоматов, совершил хищение денежных средств со счетов ряда банковских платежных карточек на территории Республики Беларусь и г. Москвы Российской Федерации, на сумму более 80 000 000 рублей, причинив материальный ущерб восьми банковским учреждениям и девяти физическим лицам, большинству из которых денежные средства были возмещены банками, клиентами которых они являлись [20].

Еще в одном случае за похожие действия, как в приведенных выше приговорах РФ и республики Беларусь, Свободненским городским судом Ф1. был приговорен по ч. 1 ст. 159, ч. 2 ст. 159 и ч. 2 ст. 159 УК РФ.

В 11 часов 00 минут Ф1 находился около здания монтажно-испытательного комплекса (МИК РН), расположенного на территории технического комплекса космодрома «Восточный». Испытывая материальные затруднения и нуждаясь в денежных средствах, Ф1 путём обмана, при помощи услуги «Мобильный банк» решил совершить хищение денежных средств у Ф10, чтобы похищенными денежными средствами в дальнейшем распорядиться по своему усмотрению. Реализуя свой внезапно возникший преступный умысел, направленный на хищение денежных средств путём обмана, Ф1, находясь на указанном выше месте, под предлогом осуществления телефонного звонка, с целью хищения денежных средств, путём обмана, завладел мобильным телефоном марки «SONY ERICSON», принадлежащий Ф10, оборудованный сим-картой с абонентским номером --, к которому была подключена услуга «Мобильный банк». Воспользовавшись моментом, что Ф10 за его действиями не наблюдает, Ф1, осознавая общественную опасность своих действий, предвидя неизбежность наступления общественно-опасных последствий в виде причинения имущественного вреда собственнику и желая наступления этих последствий, при помощи услуги «Мобильный банк», с мобильного телефона, принадлежащего Ф10 в 11 часов 03 минуты отправил на номер «900» смс-сообщение с текстом «перевод», подтвердив намерение перевести денежные средства на счёт путём отправки кода подтверждения, поступившего в ответном смс-сообщении. В результате чего умышленно, путём обмана похитил с банковского счёта Ф10 6 000 рублей, причинив последнему ущерб на указанную сумму, после чего вернул Ф10 мобильный телефон. Осознавая, что своими преступными действиями незаконно безвозмездно обратил в свою пользу чужое имущество, Ф1 с места преступления скрылся и распорядился похищенным по своему усмотрению, чем причинил потерпевшему Ф10 ущерб в размере 6 000 рублей. [21]

Таким образом, аналогичные деяния квалифицируются разными судами неодинаково, например, преступления с использованием мобильного банка с помощью сотового телефона квалифицируются правоприменителями как кража, так и мошенничество в сфере компьютерной информации [22].

Считаем такие факты недопустимыми, так как, на наш взгляд, единообразие в квалификации преступлений является необходимым условием правового государства. Указанные деяния не должны квалифицироваться по-разному, ввиду того, что семантически и юридически понятия «кража» и «мошенничество» разнятся. По нашему мнению, преступления, рассмотренные в примерах, являются кражей и должны квалифицироваться по ст. 158 УК РФ.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Проведенный сравнительно-правовой анализ положений российского и белорусского уголовного законодательства свидетельствует о значительном сходстве понимания киберпреступлений в РФ и Белоруссии. При этом, как у российского, так и у белорусского правоприменителя при рассмотрении уголовных дел возникает ряд проблем, обусловленный неясностью толкования данного вида преступлений. В этой связи мы предлагаем следующее:

1. Исключить ст. 159.6 из УК РФ. Считаем, что данная мера поможет и белорусскому законодателю решить вопросы, возникающие у правоприменителя при квалификации хищений, совершаемых с использованием компьютерной информации.

2. Принять определенные коррекционные постановления Пленумов Верховных судов обеих стран. Считаем, что налицо отсутствие единообразного подхода в применении нормы, предусматривающей уголовную ответственность за рассматриваемые преступления. Суды дают разные правовые оценки одинаковым по своей сути деяниям, квалифицируя их либо как кражу, либо как мошенничество.

СПИСОК ЛИТЕРАТУРЫ

1. Юрий Чайка рассказал о борьбе с интернет-преступностью // Российская газета. 2017. 24 авг.
2. Генпрокуратура сообщила почти о двукратном росте числа киберпреступлений в РФ в 2018 году // ТАСС. URL: tass.ru/proisshestviya/5733551.
3. Статистика УРПСВТ за 2018 год // МВД Республики Беларусь. URL: mvd.gov.by/ru/page/upravlenie-po-raskrytiyu-prestuplenij-v-sfere-vysokih-tehnologij-upravlenie-k/stastistika-urpsvt.
4. Чекунов И.Г. Квалификация преступлений против собственности, совершаемых с использованием электронных платежных систем // Российский следователь. 2011. № 24. С. 26–28.
5. Харина Э.Н. Киберпреступления: уголовно-правовой и криминалистический аспект // Вестник университета имени О.Е. Кутафина (МГЮА). 2017. № 5. С. 164–171.
6. Айков Д.В., Сейгер К., Фонстрох У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. М.: Мир, 2014. 351 с.
7. Маслакова Е.А. Правовое регулирование уголовной ответственности за преступления в сфере компьютерной информации в Российской Федерации // Правовые вопросы связи. 2006. № 2. С. 17–20.
8. Саттаров М.О. Некоторые уголовно-правовые аспекты квалификации компьютерных преступлений //

Альманах современной науки и образования. 2015. № 10. С. 125–127.
9. Андрианов М.В. Новые способы мошенничества в УК РФ // Вестник Владимирского государственного университета. 2013. № 9. С. 15–17.
10. Елин В.М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-Информатика. 2013. № 2. С. 70–76.
11. Смолин С.В. Мошенничество в сфере компьютерной информации: проблемы толкования и применения нормы ст. 159 УК РФ // Информационное право. 2015. № 4. С. 35–39.
12. Хусяинов Т.М. Криминальная Интернет-занятость (Интернет-преступность): определение и проблемы противодействия // Уголовный Закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: материалы всероссийского круглого стола. Вып. 5. Иркутск: ФГКОУ ВПО ВСИ МВД России, 2014. С. 230–236.
13. Тарасенко М.Э. Проблема борьбы с кибепреступлениями в Российской Федерации // Закон и общество: история, проблемы, перспективы: материалы межвузовской студенческой научной конференции. Красноярск: Краснояр. гос. аграр. ун-т, 2013. С. 13–16.
14. Шумихин В.Г. Седьмая форма хищения чужого имущества // Вестник Пермского университета. Юридические науки. 2014. № 2. С. 229–233.
15. Чупрова А.Ю. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. 2015. № 5. С. 131–134.
16. Александрова И.А. Новое уголовное законодательство о мошенничестве // Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2013. № 21. С. 54–62.
17. Фадина Ю.П. Уголовно-правовая характеристика мошенничества в сети Интернет // Вестник Югорского государственного университета. 2017. № 1-2. С. 117–121.
18. Обвинительный приговор судебного участка № 134 Юрлинского муниципального района № 1-2 от 01.02.2018 // Росправосудие.
URL: rospravosudie.ru/court-sudebnyj-uchastok-134-yurlinskogo-municipalnogo-rajona-s/act-241154020/.
19. Обвинительный приговор Дмитровградского городского суда по делу 1-243 от 11.08.2017 // Росправосудие.
URL: rospravosudie.com/court-dimitrovgradskij-gorodskoj-sud-ulyanovskaya-oblast-s/act-558724770/.
20. Определение судебной коллегии по уголовным делам Витебского областного суда от 9 декабря 2014 года // Верховный суд Республики Беларусь: интернет-портал судов общей юрисдикции.
URL: court.gov.by/justice/press_office/d4d8701ef73d975f.html.
21. Обвинительный приговор Свободненского городского суда по делу 1-330/2016 года // Росправосудие.
URL: rospravosudie.com/court-svobodnenskij-gorodskoj-sud-amurskaya-oblast-s/act-533552056/.
22. Хачатурова С.С. Хранение и защита информации // Международный журнал прикладных и фундаментальных исследований. 2016. № 2-1. С. 63–65.

REFERENCES

1. Yury Chaika told about the Internet-crime prevention. *Rossiyskaya gazeta*, 2017, 24 August.
2. General Procuracy reported on about double growth of the number of cyber-crimes in the RF in 2018. *TASS*. URL: tass.ru/proisshestviya/5733551.
3. Statistical data of the Department for Uncovering Crimes in high-tech for 2018. *MVD Respubliki Belarus*. URL: mvd.gov.by/ru/page/upravlenie-po-raskrytiyu-prestuplenij-v-sfere-vysokih-tehnologij-upravlenie-k/stastistika-urpsvt.
4. Chekunov I.G. Classification of crimes against property committed using electronic payment systems. *Rossiyskiy sledovatel*, 2011, no. 24, pp. 26–28.
5. Kharina E.N. Cyber-crimes: criminal law and criminalistics aspects. *Vestnik universiteta imeni O.E. Kutafina (MGYuA)*, 2017, no. 5, pp. 164–171.
6. Aykov D.V., Seyger K., Fonstrokh U. *Kompyuternye prestupleniya. Ru-kovodstvo po borbe s kompyuternymi prestupleniyami* [Computer crimes. Guidance on computer crimes prevention]. Moscow, Mir Publ., 2014. 351 p.
7. Maslakova E.A. Legal regulation of criminal liability for cyber crimes. *Pravovye voprosy svyazi*, 2006, no. 2, pp. 17–20.
8. Sattarov M.O. Certain criminal and legal aspects of qualifying computer crimes. *Almanakh sovremennoy nauki i obrazovaniya*, 2015, no. 10, pp. 125–127.
9. Andrianov M.V. New methods of fraud in Criminal Code of the RF. *Vestnik Vladimirskogo gosudarstvennogo universiteta*, 2013, no. 9, pp. 15–17.
10. Elin V.M. Computer-related fraud as a new offense in the Russian law. *Biznes-Informatika*, 2013, no. 2, pp. 70–76.
11. Smolin S.V. Computer Fraud (Section 159 of the Criminal Code of the Russian Federation): problems of interpretation and application. *Informatsionnoe pravo*, 2015, no. 4, pp. 35–39.
12. Khusyainov T.M. Criminal Internet-activity (Internet-crime): definition and the problems of countering. *Ugolovnyy Zakon Rossiyskoy Federatsii: problemy pravoprimeneniya i perspektivy sovershenstvovaniya: materialy vserossiyskogo kruglogo stola*. Irkutsk, FGKOU VPO VSI MVD Rossii Publ., 2014. Vyp. 5, pp. 230–236.
13. Tarasenko M.E. The problems of cyber-crimes prevention in the Russian Federation. *Zakon i obshchestvo: istoriya, problemy, perspektivy: materialy mezhvuzovskoy studencheskoy nauchnoy konferentsii*. Krasnoyarsk, Krasnoyar. gos. agrar. un-t Publ., pp. 13–16.
14. Shumikhin V.G. The seventh form of theft of property. *Vestnik Permskogo universiteta. Yuridicheskie nauki*, 2014, no. 2, pp. 229–233.
15. Chuprova A.Yu. The problems of classification of fraud related to use of information technologies. *Ugolovnoe pravo*, 2015, no. 5, pp. 131–134.
16. Aleksandrova I.A. New criminal legislation about fraud. *Yuridicheskaya nauka i praktika. Vestnik Nizhegorodskoy akademii MVD Rossii*, 2013, no. 21, pp. 54–62.
17. Fadina Yu.P. Criminal-legal characteristic of fraud on the internet. *Vestnik Yugorskogo gosudarstvennogo universiteta*, 2017, no. 1-2, pp. 117–121.

18. Judgment of guilt of court circuit No. 134 of Yurlinsk municipal district No. 1-2 dated the 01.02.2018. *Rospravosudie*. URL: rospravosudie.ru/court-sudebnyj-uchastok-134-yurlinskogo-municipalnogo-rajona-s/act-241154020/.
19. Judgment of guilt of Dmitrovgrad city court on the case 1-243 dated the 11.08.2017. *Rospravosudie*. URL: rospravosudie.com/court-dimitrovgradskij-gorodskoj-sud-ulyanovskaya-oblast-s/act-558724770/.
20. The decision of the judicial division for criminal cases of Vitebsk district court dated the 9th of December 2014. *Verkhovnyy sud Respubliki Belarus: internet-portal sudov obshchey yurisdiktsii*. URL: court.gov.by/justice/press_office/d4d8701ef73d975f.html.
21. Judgment of guilt of Svobodnensk city court on the case 1-330/2016. *Rospravosudie*. URL: rospravosudie.com/court-svobodnenskij-gorodskoj-sud-amurskaya-oblast-s/act-533552056/.
22. Khachaturova S.S. Storage and data protection. *Mezhdunarodnyy zhurnal prikladnykh i fundamentalnykh issledovaniy*, 2016, no. 2-1, pp. 63–65.

CRIMINAL POLICY OF RUSSIA IN THE SPHERE OF CYBERCRIME PREVENTION: RATHER-LEGAL ANALYSIS

O.Yu. Savelyeva, PhD (Law), Associate Professor, assistant professor of Chair "Criminal Law and Procedure"
K.A. Zaburdaeva, lecturer of Chair "Criminal Law and Procedure"
D.N. Medinovskaya, graduate student of Chair "Criminal Law and Procedure"
Togliatti State University, Togliatti (Russia)

Keywords: cybercrimes; cyber security; cyber fraud; computer fraud; computer information; electronic payment facilities.

Abstract: The dynamic and continuous process of information development followed by the appearance of new digital infrastructures, computer engineering, and digital communication technologies, on the one hand, positively influences all spheres of human activity promoting the improvement of life quality. On the other hand, these processes have negative consequences as well. In recent years, the number of thefts committed not in the traditional way but with the help of various products of technological and information progress (for example, through the Internet). Consequently, law enforcement authorities across the globe faced a new negative social phenomenon – cybercrime.

The authors carried out rather-legal analysis both of Russian and Belorussian legislation and case materials of two countries. Therewith, close attention is paid to the study of cyber fraud. The authors analyzed both the opinions of many Russian and Belorussian scientists concerning the understanding of a term "cybercrime" and the statistical data on the state of cybercrime for the period of 2016–2018 and assessed these data. The obtained data allows concluding about the negative criminological dynamics of cybercrimes both in Russia and in the territory of Belarus, about the intensive growth of some types of cybercrimes (cyber fraud and fraud committed using electronic payment facilities; other crimes committed through the Internet), as well as about the imperfection of crime policy in regards to the cybercrimes prevention. The authors suggest re-evaluating the provisions of criminal legislation in regards to the regulation of the responsibility for some types of cybercrimes, as well as re-confirming the position of the RF Supreme Court on the issues of considering actions committed in cyberspace as a definite type of thefts.