УДК 343.7

А. А. Куликова

Институт сферы обслуживания и предпринимательства (филиал) ДГТУ
в г. Шахты, Шахты, e-mail: vanurkina@yandex.ru

А. И. Асташова

Институт сферы обслуживания и предпринимательства (филиал) ДГТУ
в г. Шахты, Шахты, e-mail: astashova81@yandex.ru

ЗАЩИТА СОБСТВЕННОСТИ УГОЛОВНО-ПРАВОВЫМИ СРЕДСТВАМИ В ЦИФРОВУЮ ЭПОХУ

Ключевые слова: кража, совершенная с банковского счета, а равно в отношении электронных денежных средств, мошенничество с использованием электронных средств платежа, постановление Пленума Верховного Суда РФ, хищение, обман, злоупотребление доверием, банковский счет, электронные средства платежа.

В настоящее время общественные отношения испытывают значительное влияние технического прогресса. Цифровизация общественных отношений, несмотря на ее неоспоримые достоинства, порождает новые способы совершения преступных деяний. Реакцией законодателя на обозначенные обстоятельства является, в том числе изменение редакций статей 158, 159.3, 159.6 УК РФ. Данные новеллы вызвали множество затруднений у правоприменителей, дискуссии в научном сообществе и ошибки в судебной практике. В данной статье автором представлен анализ указанных норм уголовного законодательства с учетом положений постановления Пленума Верховного Суда РФ от 29.06.2021 № 22. Проведенный анализ показал, что Пленум Верховного Суда РФ за период действия рассматриваемых правовых норм изменил свою позицию в противоположную сторону. То есть, деяние, которое согласно постановлению от 30.11.2017 № 48 рекомендовано было квалифицировать как мошенничество с использованием электронных средств платежа, теперь в соответствии с положениями постановления Пленума Верховного Суда РФ от 27.12.2002 № 29 в новой редакции, следует квалифицировать как кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств. Кроме того на сегодняшний день отсутствует ясность в отношении того что, какие деяния являются преступными в соответствии с диспозицией ст. 159.3 УК РФ. Данными обстоятельствами обусловлена сложившаяся противоречивая судебная практика по привлечению к ответственности за рассматриваемые деяния, что влияет на важнейшие принципы уголовного права – справедливость и неотвратимость наказания. Учитывая вышесказанное, в статье предложено решеные указанных и иных вопросов, связанных с хищением «электронных» денежных средств. В работе также представлен анализ зарубежных источников по теме исследования.

A. A. Kulikova

Institute of Service and Entrepreneurship (Branch) of the Don State Technical University
in Shakhty, Shakhty, e-mail: vanurkina@yandex.ru

A. I. Astashova

Institute of Service and Entrepreneurship (Branch) of the Don State Technical University
in Shakhty, Shakhty, e-mail: astashova81@yandex.ru

PROTECTION OF PROPERTY BY CRIMINAL LEGAL MEANS IN THE DIGITAL AGE

Keywords: theft from a bank account, as well as with electronic money, fraud using electronic means of payment, a resolution of the Plenum of the Supreme Court of the Russian Federation, theft, deception, abuse of trust, bank account, electronic means of payment.

Today public relations are significantly influenced by technological progress. Despite of undeniable advantages digitalization of public relations generates new ways of committing criminal acts. The reaction of the legislator to the indicated circumstances is a change in the wording of Articles 158, 159.3, 159.6 of the Criminal Code of the Russian Federation. These novels caused a lot of difficulties for law enforcement officers, discussions in the scientific community and errors in judicial practice. In this article the author presents an analysis of these norms of criminal legislation taking into account the provisions of the resolution of the Plenum of the Supreme Court of the Russian Federation N 22 of 29 June, 2021. The analysis showed that the Plenum of the Supreme Court of the Russian Federation changed its position in the opposite direction during the period of validity of the legal norms under consideration. The act according to the resolution of

November 30, 2017 N 48 was recommended to qualify as fraud using electronic means of payment, now in accordance with the provisions of the resolution of the Plenum of the Supreme Court of the Russian Federation of December, 2002 N 29 in the new edition, should be qualified as theft from a bank account, as well as in relation to electronic money. In addition, there is no clarity as to what acts are criminal in accordance with the disposition of Article 159.3 of the Criminal Code of the Russian Federation. These circumstances are due to the current contradictory judicial practice on bringing to justice for the acts in question, which affects the most important principles of criminal law – justice and the inevitability of punishment. Taking into account the above, the article suggests solving these and other issues related to the theft of "electronic" funds.

Введение

Общественные отношения в современном мире испытывают значительное влияние со стороны стремительно развивающихся технологий. Все больше сфер общественной жизни переход в цифровую реальность, в связи с чем в виртуальном пространстве оказывается большой объем различной информации, которая является предметом различных правовых отношений. Так, например, различные данные могут быть предметом отношений, связанных с защитой персональных данных, государственной, коммерческой, врачебной и иных видов тайн, охраняемых законом, частью личной жизни человека, интеллектуальной собственностью и др. Перечисленные отношения входят в предмет правового регулирования и охраняются от посягательств на них различными средствами правовой защиты. Кроме того, цифровая информация может быть средством, используемым для достижения преступного результата. В связи с чем, появляется необходимость правового регулирования и защиты возникающих отношений в связи с цифровизацией общества.

Принимая во внимание изменения, происходящие в обществе, появление общественных отношений, требующих уголовно-правовой охраны и новых видов посягательства на собственность федеральным законом от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» [1] дополнены ч.3 статьи 158 УК РФ «Кража» пунктом «г», устанавливающем ответственность за совершение кражи с банковского счета, а равно в отношении электронных денежных средств. Этим же законом изменена редакция статьи 159.3 «Мошенничество с использованием платежных карт» где изменился предмет преступления «платежные карты» на «электронные средства платежа». Также изменениям подверглась ч. 3 статья 159.6 «Мошенничество в сфере компьютерной информации» – внесен п. «в» устанавливающий ответственность за мошенничество в сфере компьютерной информации, то есть 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, или то же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину совершенные с банковского счета, а равно в отношении электронных денежных средств.

Вышеназванные нововведения вызвали дискуссию среди ученых. Данные изменения восприняты неоднозначно ученым сообществом, так как отсутствует ясность в понимании признаков реформируемых составов преступлений.

Проблеме применения на практике положения, закрепленных статьями 158 (п. «г» ч. 3), 159.3 уделяли внимание различные ученые, среди которых можно отметить работы В.И. Тюнина, Ю.И. Степанова [2], П.С. Яни [3, 4], Е.Н. Олейник [5], М.А. Филатовой [6], А.П. Перетолчина [7], А.В. Архипова [8], Т.Н. Долгих [9], А.К Клименко [10], Е.А. Русскевич [11]. В своих работах данные авторы подчеркивали сложность квалификации деяний по статьям Уголовного кодекса РФ, введенным федеральным законом от 23.04.2018 № 111-ФЗ. Однако, так или иначе авторы соглашались с разъяснениями Пленума Верховного Суда от 30.11.2017 № 48 [12]. Ситуация изменилась с принятием постановления Пленума Верховного Суда РФ от 29.06.2021 № 22 [13]. Те деяния, которые ранее квалифицировались, как мошенничество с использование электронных средств платежа надлежит оценивать как кражу совершенную с банковского счета, а равно в отношении электронных средств платежа. В связи с чем, указанные изменения не только не сняли ранее возникших вопросов, но еще и породили новые. Так, например, остается неясным ка-

кие деяния подпадают под сферу действия ст. 159.3 УК РФ и как отграничить признаки ст. 159.3 от ст. 159.6 УК РФ? Перетолчин А.П. пришел к выводу, что в свете обновленных рекомендации Пленума Верховного Суда РФ деяния, при которых лицо осуществляло оплату поддельным или принадлежащим другому лицу электронными средствами платежа товаров и услуг при участии уполномоченного специалиста организации, необходимо квалифицировать как мошенничество [7]. Его позиция исходит из анализа направленности совершенного обмана на уполномоченного специалиста организации. Однако такая позиция не отличается от ранее сформированной, которую и Верховный Суд РФ и Конституционный Суд РФ признал ошибочной. Данный автор не раскрыл в статье признаки уполномоченного лица, которое, по его мнению, должно присутствовать при оплате товара при помощи электронных средств платежа, а также, н наш взгляд, ошибочно считает осуществление бесконтактной оплаты посредством прикладывания средства платежа активным обманом сотрудника торговой организации. С учетом вышесказанного считаем актуальным пересмотреть подход к квалификации исследуемых деяний и законодательному закреплению запрета хищений с использованием электронных средств платежа.

Целью проведенного исследования является анализ возможностей уголовного законодательства России противостоять совершению хищений с банковского счета, а равно совершенных с использованием электронных средств платежа.

Материал и методы исследования

В работе исследованы изменения уголовного законодательства, произошедшие в связи с реакцией законодателя на появление новых способов преступных посягательств на собственность; рассмотрены рекомендации Пленума Верховного Суда РФ, содержащиеся в постановлениях относительно квалификации названных преступных посягательства; проведен анализ материалов судов общей юрисдикции по рассматриваемой категории дел; изучена позиция Конституционного Суда, содержащаяся в определении Конституционного Суда РФ от 09.07.2021 № 1374-О [14]; исследованы научные труды, посвященные проблемам ответственности за хищения, совершаемые с банковского счета, а также совершенные с использованием электронных средств платежа; рассмотрена позиция зарубежного законодателя относительно квалификации рассматриваемых деяний; предложена авторская редакция новой статьи Уголовного кодекса Российской Федерации, принятие которой решило бы существующие проблемы правоприменения в данной сфере.

При проведении исследования основополагающим методом стал диалектический метод познания действительности. Кроме того, мы использовали методы анализа и синтеза, формально-правовые и сравнительно-правовые методы.

Результаты исследования и их обсуждение

Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» [15] было дополнено постановлением Пленума Верховного Суда РФ от 29.06.2021 № 22 «О внесении изменений в отдельные постановления Пленума Верховного Суда Российской Федерации по уголовным делам» пунктами 25.1-25.4, 26 которые содержат разъяснения о применении п. «г» ч.3 ст. 158 УК РФ. Так, Пленум рекомендует квалифицировать деяния по данному пункту, если лицо тайно похитило денежные средства, находящиеся на банковском счете жертвы, воспользовавшись банковской картой, иными средствами безналичного платежа, в том числе при помощи функции безналичной оплаты, используя персональную, контрольную информацию, ПИН-код и другие данные.

Необходимо отметить, что диспозиция п. «г» ч.3 т. 158 УК РФ является отсылочной и применяется в том случае, если совершенные деяния не могут быть квалифицированы по ст. 159.3 УК РФ, иначе говоря, при отсутствии признаки мошенничества с использованием электронных средств платежа. Следовательно, рассматриваемые нормы являются конкурирующими и вызывают сложности у правоприменителя. Поэтому, для правильной квалификации исследуемых деяний следует уяснить признаки преступления, предусмотренного ст. 159.3 УК РФ.

В диспозиции новой редакции ст. 159.3 не описаны признаки мошенничества с использованием электронных средств платежа. Поэтому, для определения признаков данного деяния обратимся к разъяснениям Пленума Верховного Суда от 30.11.2017

№ 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». В ранее действовавшей редакции правоприменителю при квалификации деяния по ст. 159.3, предлагалось принимать во внимание то обстоятельство, что если обман не направлен непосредственно на завладение чужим имуществом, а используется только для облегчения доступа к нему, действия виновного в зависимости от способа хищения образуют состав кражи или грабежа. Постановлением Пленума Верховного Суда РФ от 29.06.2021 № 22 данные положения исключены.

Анализ положений постановлений Пленума Верховного Суда РФ показывает, что проблемы квалификации кражи с банковского счета, а равно в отношении электронных денежных средств и ограничения ее от мошенничества с использованием электронных средств платежа в правоприменительной практике остаются не решенными, несмотря на произведенные преобразования. И если, постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» дополнено разъяснениями в отношении того, какое деяние следует квалифицировать по п. «г» ч.3 ст. 158 УК РФ, то изменения, внесенные в постановление Пленума Верховного Суда от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» в отношении определения мошенничества с использованием электронных средств платежа оставляют вопрос открытым.

Согласно ранее действовавшей редакции постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» основное отграничение кражи банковского счета, а равно в отношении электронных денежных средств от мошенничества с использованием электронных средств платежа состояло в направленности обмана. Так, обман должен был быть направлен на уполномоченного работника кредитной, торговой или иной организации и состоять в ложных сведениях о принадлежности указанному лицу такой карты на законных основаниях либо путем умолчания о незаконном владении им платежной картой. Такого мнения трактовки положений законодательства придерживаются и ученые. На сегодняшний день отсутствует единое понимание того, какое деяние следует признавать мошенничеством с использованием электронных средств платежа, чему способствует исключение соответствующих разъяснений из постановления Пленума Верховного Суда РФ.

В период действия норм, введенных ФЗ от 23.04.2018 № 111-ФЗ произошли значительные изменения в отношении определения признаков рассматриваемых деяний. Так, согласно определении Конституционного Суда РФ от 09.07.2021 № 1374-О «О прекращении производства по делу о проверке конституционности пункта «г» части третьей статьи 158 и статьи 159.3 Уголовного кодекса Российской Федерации в связи с запросом Железнодорожного районного суда города Рязани» «использование обладателем чужой платежной карты обмана (злоупотребления доверием) для введения в заблуждение уполномоченного работника организации, реализующей товары, выполняющей работы, предоставляющей услуги относительно принадлежности платежной карты не может рассматриваться как мошенничество (покушение на мошенничество), поскольку указанный работник не наделен распорядительными полномочиями в отношении денежных средств на конкретном банковском счете». Такой обман может быть расценен только как средство достижения цели – тайного хищения чужого имущества.

Приведем несколько примеров уголовно-правовой оценки деяния из материалов судебной практики судов общей юрисдикции.

1. Квалификация перевода денежных средств через мобильное приложение на определенный расчетный счет с использованием мобильного телефона взятого для совершения звонка, производится по п. «г» ч. 3 ст. 158 УК РФ [16].

2. Судебная коллегия по уголовным делам Верховного Суда Российской Федерации оставила без изменения приговор, в котором суд квалифицировал деяние, совершенное при обстоятельствах, когда владелец банковской карты передал виновному банковскую карту и попросил снять 10 000 рублей, сообщив пин-код карты, а виновный, не имея каких-либо полномочий на распоряжение денежными средствами на банковском счете потерпевшего, тайно похитил хранившиеся там денежные средства, сняв с использованием данной банковской карты через банкомат 40 тысяч рублей, а также осуществив через банкомат переводы денежных средств в сумме 40 тысяч рублей и 20 тысяч рублей

своим знакомым как кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств [17].

3. Уголовно-правовая квалификация совершения бесконтактной оплаты товара, услуг чужой банковской карты в сложившейся правоприменительной практике производится по части первой статьи 159.3 УК Российской Федерации, что в свете последних изменений, внесенных в постановления Пленума Верховного Суда РФ является не правильным и влечет переквалификацию по п. «г» ч. 3 ст. 158 УК РФ. (Постановление Чертковского районного суда № 1-95/2020 от 27 ноября 2020 г. по делу № 1-95/2020 [18]; Постановление Волгодонского районного суда № 1-588/2020 от 15 октября 2020 г. по делу № 1-588/2020 [19]; Постановление Волгодонского районного суда № 1-589/2020 от 7 октября 2020 г. по делу № 1-589/2020 [20] и др.)

В соответствии с положениями уголовного законодательства обязательным признаком кражи является совершение хищения *тайно*, обязательным признаком мошенничества является завладение чужим имуществом путем *обмана или злоупотребления доверием*. Если обратиться к выше приведенным примерам, то мы увидим противоречивую ситуацию, когда в первом случае виновным был *обманут* собственник телефона (т.е. телефон у потерпевшего взяли под предлогом совершения звонка) и похищены денежные средства путем совершения перевода – деяние квалифицировано как кража, в случае, когда карта была и похищена или найдена и виновный *тайно* расплатился данной карты посредством бесконтактной оплаты – деяние квалифицируется как мошенничество.

В качестве примера затруднения при квалификации рассматриваемых преступлений приведем определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 № 12-УДП20-5-К6. Согласно данном акту виновный нашел банковскую карту с функцией безналичной оплаты на улице, после чего производил оплату товаров и услуг данной картой в результате чего потрепевшей был нанесен ущерб в размере 3025 руб. Суд первой и апелляционной инстанции квалифицировали данное деяние по п «г» ч. 3 ст. 158 УК РФ. Шестой кассационный суд общей юрисдикции изменил приговор, переквалифицировал действия осужденного на ч. 1 ст. 159.3 УК РФ. Определением Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 № 12-УДП20-5-К6 определение кассационной инстанции было отменено в связи с не правильной юридической квалификацией действий виновного с учетом положений действующего уголовного закона [21].

Постановление Пленума Верховного Суда РФ от 29.06.2021 № 22 «О внесении изменений в отдельные постановления Пленума Верховного Суда Российской Федерации по уголовным делам» должно было решить обозначенные проблемы, возникающие при квалификации исследуемых преступлений.

Можно согласиться с тем, что внесение дополнения в постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» внесло ясность в определение понятия и признаков кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств. Однако остались не решенными вопросы относительно определения понятия и признаков мошенничества с использованием электронных средств платежа. В данном ключе встает вопрос о необходимости декриминализации ст. 159.3 УК РФ в связи с отсутствием понимания объективной стороны данного состава даже на уровне разъяснений Пленума Верховного Суда РФ. Тем более, что ч. 3 статьи 159.6 предусматривает ответственность за мошенничество в сфере компьютерной информации, то есть 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, или то же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину совершенные с банковского счета, а равно в отношении электронных денежных средств.

Также интересен вопрос о наличии иных форм хищения или завладения средствами, находящимися на банковском счете, или же при применении электронных средств платежа. Например, если при совершении грабежа предметом открытого хищения являются документы, содержащие сведения, при

помощи которых грабитель получает доступ к лицевому счету потерпевшего и осуществляет операции по переводу денежных средств используя электронные средства платежа, будет ли такое деяние квалифицировано как грабеж? Или же, если преступник путем шантажа требует передать ему контрольную информацию и распоряжается электронными денежными средствами жертвы, можно ли считать такое деяние вымогательством? И если ответить на заданные вопросы положительно, то необходимо также добавлять в ст. 161, 163 УК РФ соответствующие квалифицированные составы.

Такое решение обозначенных проблем не считаем успешным. Чрезмерное загромождение Уголовного Кодекса смежными составами преступлений, препятствует однообразному применению уголовного закона и способствует различному его толкованию, что и подтверждается приведенными выше доводами. Представляется более предпочтительным исключение из текста УК РФ п. «г» ч.3 статьи 158 УК РФ и ст. 159.3 и введение новой статьи «Хищение, совершенное с банковского счета, а равно в отношении электронных денежных средств». В данной статье необходимо дифференцировать ответственность в зависимости от формы совершаемого хищения.

При детальном анализе преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ обнажается еще одна проблема, которая нами ранее уже была обозначена [22]. На наш взгляд, не соответствует принципу справедливости то обстоятельство, что размер похищенных денежных средств с банковского счета, а равно в отношении электронных денежных средств не указан в качестве обязательного признака при квалификации данного деяния. Считаем ошибочным признание равной степени общественной опасности кражи с банковского счета, а равно в отношении электронных денежных средств с кражей, совершенной с незаконным проникновением в жилище, кражей из нефтепровода, нефтепродуктопровода, газопровода и кражей в крупном размере. В такой ситуации наказание за оплату чужой банковской картой покупки на сумму, например, 2000 руб. должно быть назначено наказание соразмерное краже совершенной в крупном размере.

В определении от 09.07.2021 № 1374-О Конституционный Суд РФ в отношении несовпадения санкций и категорий преступлений, предусмотренных пунктом «г» части третьей статьи 158 и частью первой статьи 159.3 УК Российской Федерации пояснил, что не усматривает в данном случае несоразмерности, которая предполагала бы необходимость конституционной оценки оспариваемых положений в этом аспекте с учетом того, что хищение денежных средств с банковского счета или электронных денежных средств не только посягает на собственность, но и может подрывать доверие к безналичным способам хранения денежных средств и ведению расчетов, которые являются важным элементом устойчивого функционирования современной экономики. То есть, тем самым Конституционны Суд РФ объясняет правомерность отягчения уголовной ответственности дополнительным объектом посягательства – *доверии к безналичным способам хранения денежных средств и ведению расчетов*. Что также вызывает сомнения, поскольку обозначенные в определении отношения не являются объектом уголовно-правовой охраны и не закреплены в качестве признака, отягчающего наказание в ст. 63 УК РФ.

Считаем, что вопросы справедливости наказания и соотносимости размера уголовного наказания и степени общественной опасности кражи совершенной с банковского счета, а равно в отношении электронных денежных средств заслуживают отдельного исследования.

Проблема хищений электронных денежных средств является транснациональной. Такое хищение в зарубежных странах определяется как «банковское мошенничество» [23], «компьютерное мошенничество» [24]. Компьютерное мошенничество является результатом иных неправомерных действий, например, мошенники получают доступ к средствам держателей карт после взлома, фишинга или скимминга, направленного на кражу данных банковской карты [25]. Совершая хищения при помощи мобильных телефонов, жертвы лишаются денежных средств после звонков злоумышленников, в которых часто применяются методы фишинга для кражи информации потерпевших [26]. Поэтому в некоторых ситуациях телефонные мошенничества могут быть известны как “голосовой фишинг” или “вишинг” [27]. Фишинг представляет собой какие-то массовые рассылки писем или уведомлений на почты от имени известных брендов, банков, платежных систем, почто-

вых сервисов, социальных сетей, доверие к которым однозначно заложено в мышлении пользователя сети. В письме из рассылки часто содержится прямая ссылка на сайт который сложно отличить от оригинального [28]. Скимминг предполагает электронное сканирование платежной карты потерпевшего, как правило, в целях последующего хищения денежных средств, находящихся на банковском или ином счете, к которому привязана эта платежная карта [29].

Кибер-мошенничество стало глобальной угрозой из-за широкого применения информационных компьютерных технологий [30]. Беспрецедентная революция в области информационных компьютерных технологий позволила дистанционно совершать кибер-мошенничество с помощью Интернета и беспроводной связи [31]. Один из видов компьютерного мошенничества, мошенничество с банковскими картами, например, привело к глобальным потерям в размере более 27 миллиардов долларов США в 2018 году и, по прогнозам, достигнет более 35 миллиардов долларов США к 2023 году [32].

В США Федеральный закон [33] дает очень широкое определение банковского мошенничества. Он охватывает любую «схему или уловку», предназначенную для «обмана финансового учреждения» или использование обманных средств в целях получения ценностей, которыми финансовое учреждение владеет или контролирует. За совершение банковского мошенничества в соответствии с федеральным законодательством США предусмотрено наказание – тюремное заключение на срок до 30 лет, и/или штраф до 1 миллиона. Под «финансовым учреждением» в соответствии с законодательством понимаются банки и кредитные организации, застрахованные на федеральном уровне, такие как Федеральная корпорация вкладов (FDIC), Федеральные резервные банки компании, занимающиеся ипотечным кредитованием, и некоторые другие учреждения. Законы штатов по-разному квалифицируют банковское мошенничество.

Согласно данным Европола мошенничество с платежными картами, представляющее низкорисковую и высокодоходную преступную деятельность, можно разделить на два различных типа: мошенничество без предъявления карты, которое совершается в основном в Интернете, и мошенничество с помощью карты, которое обычно совершается в торговых организациях и банкоматах.

Как форма киберпреступности мошенничество с использованием электронных средств платежа является одним из приоритетов EMPACT, главных направлений работы Европола в рамках политического цикла ЕС 2018-2021 гг.

Мошенничество без предъявления включает несанкционированное использование данных кредитных или дебетовых карт (номер карты, адрес выставления счета, защитный код и срок действия) для покупки продуктов и оплаты услуг без личного присутствия, например, через электронную почту, коммерческие сайты или по телефону. В большинстве случаев жертвы не знают о несанкционированном использовании своих карт, которые находятся у них.

Этот вид незаконной деятельности, часто называемый кардингом. Он неуклонно растет посредством утечки данных, при помощи использования и распространения вредоносных компьютерных программ, предназначенных для кражи данных, а также инструментов фишинга [34].

Как видно из приведенных примеров, проблема борьбы хищениями, совершаемыми при помощи современных компьютерных, информационных технологий является актуальной для всего мира. Рассматриваемые преступления являются транснациональными. Национальное законодательство зарубежных государств содержит нормы, предусматривающие уголовную ответственность за хищения электронных денежных средств. Анализ научных зарубежных публикаций показал, что такое хищение определяется как «банковское мошенничество», «компьютерное мошенничество», «кардинг», как одна из форм киберпреступности.

В зарубежных странах посягательство на денежные средства, находящиеся на банковском счете, а равно осуществленные с использованием электронных средств платежа признают мошенничеством независимо от направленности обмана и других факторов.

Заключение

На основании проведенного анализа законодательства Российской Федерации, постановлений Пленума Верховного Суда РФ, материалов судебной практики нами сформулирован иной подход к установлению уголовной ответственности за хищения, совершенные с использованием электронных средств платежа.

Проведенное исследование показало, что принятые законодателем меры уголовной ответственности за хищение, совершенное с использованием электронных средств платежа, а также с банковского счета не являются эффективными, поскольку неоднозначно трактуются правоприменительными органами, отсутствует ясность и точность формулировок, уголовный закон излишне загружен смежными составами преступлений. На основании выводов, полученных в процессе решения поставленных исследовательских задач нами предпринята попытка структурировать различные виды хищения совершенного с использованием электронных средств платежа, а также с банковского счета в одной статье, установив повышенную меру уголовной ответственности в зависимости от способа такого хищения.

Предлагаемая редакция ст.164.1 «Хищение, совершенное с банковского счета, а равно в отношении электронных денежных средств»:

1. Тайное хищение, совершенное с банковского счета, а равно в отношении электронных денежных средств – наказывается…

2. Хищение, совершенное с банковского счета, а равно в отношении электронных денежных средств путем обмана или злоупотребления доверием – наказывается…

3. Открытое хищение, совершенное с банковского счета, а равно в отношении электронных денежных средств – наказывается…

4. Требование передачи данных, для предоставления права распоряжаться средствами с банковского счета, электронными денежными средствами под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких – наказывается…

Библиографический список

1. Федеральный закон от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // Собрание законодательства РФ. 2018. № 18. Ст. 2581.

2. Тюнин В.И., Степанов Ю.И. Кража с банковского счета, а равно в отношении электронных денежных средств (криминализация и квалификация преступления) // Российский следователь. 2021. № 3. С. 41-45. DOI: 10.18572/1812-3783-2021-3-41-45.

3. Яни П.С. Хищение с использованием чужой банковской карты в магазине следует квалифицировать как мошенничество // Законность. 2020. № 12. С. 39-43.

4. Яни П. Мошенничество с использованием электронных средств платежа // Законность. 2019. № 4-7.

5. Олейник Е.Н. Проблема отграничения кражи имущества с банковского счета от мошенничества с использованием электронных средств платежа // Балтийский гуманитарный журнал. 2018. Т. 7. № 2 (23).

6. Филатова М.А. Хищение с использованием чужой банковской карты в магазине образует состав кражи // Законность. 2020. № 12. С. 34-38.

7. Перетолчин А.П. Некоторые проблемы квалификации мошенничества с использованием электронных средств платежа // Алтайский юридический вестник. 2019. № 4(28). С. 71-77.

8. Архипов А. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства // Уголовное право. 2018. № 3.

9. Долгих Т.Н. Ответственность за хищение денежных средств с банковской карты. Доступ из справ.-правовой системы «КонсультанПлюс» (дата обращения 20.11.2021).

10. Клименко А.К. Хищения безналичных и электронных денежных средств: вопросы квалификации // Российский следователь. 2020. № 5. С. 38-42. DOI: 10.18572/1812-3783-2020-5-38-42.

11. Русскевич Е.А. Отграничение кражи с банковского счета или в отношении электронных денежных средств от смежных составов преступлений // Уголовное право. 2019. № 2. С. 59-64.

12. Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Российская газета. 2017. № 280.

13. Постановление Пленума Верховного Суда РФ от 29.06.2021 № 22 «О внесении изменений в отдельные постановления Пленума Верховного Суда Российской Федерации по уголовным делам» // Российская газета. 2021. № 159.

14. Определение Конституционного Суда РФ от 09.07.2021 № 1374-О «О прекращении производства по делу о проверке конституционности пункта «г» части третьей статьи 158 и статьи 159.3 Уголовного кодекса Российской Федерации в связи с запросом Железнодорожного районного суда города Рязани. Доступ из справ.-правовой системы «КонсультанПлюс» (дата обращения 20.11.2021).

15. Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» // Бюллетень Верховного Суда РФ. 2003. № 2.

16. Приговор Неклиновского районного суда № 1-220/2020 от 23 июля 2020 г. по делу № 1-220/2020 // Интернет-ресурс Судебные и нормативные акты РФ. URL: sudact.ru/regular/doc/VdeBUBauVJ6j/ (дата обращения 20.11.2021).

17. Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 25.02.2021 N 81-УД21-1-К8. Доступ из справ.-правовой системы «КонсультанПлюс» (дата обращения 20.11.2021).

18. Интернет-ресурс Судебные и нормативные акты РФ. URL: sudact.ru/regular/doc/ccdAZaHL7fxQ/ (дата обращения 20.11.2021).

19. Интернет-ресурс Судебные и нормативные акты РФ. URL: sudact.ru/regular/doc/uSxwUxGU3RdN/ (дата обращения 20.11.2021).

20. Интернет-ресурс Судебные и нормативные акты РФ. URL: sudact.ru/regular/doc/dHnSNUws0Z8/ (дата обращения 20.11.2021).

21. Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 N 12-УДП20-5-К6. Доступ из справ.-правовой системы «КонсультанПлюс» (дата обращения 20.11.2021).

22. Куликова А. А. Вопросы уголовной ответственности за преступные посягательства на электронные денежные средства и электронные средства платежа // Актуальные проблемы применения уголовного законодательства: Сборник материалов Международной научно-практической конференции, Ростов-на-Дону, 21 мая 2020 года / Отв. редактор Н.С. Сорокун. Ростов-на-Дону: Ростовский юридический институт Министерства внутренних дел Российской Федерации, 2020. С. 115-120.

23. Bossler A.M., Berenblum T. Introduction: New directions in cybercrime research. J Crime Justice. 2019. № 42. P. 495–499. DOI:10.1080/0735648X.2019.1692426.

24. Van Nguyen T. The modus operandi of transnational computer fraud: a crime script analysis in Vietnam. Trends Organ Crim. 2021. DOI:10.1007/s12117-021-09422-1.

25. Peretti K. Data breaches: What the underground world of carding reveals. Santa Clara High Technol Law J. 2008. № 25. P. 375–413.

26. Choi K., Lee J., Chun Y. (2017) Voice phishing fraud and its modus operandi. Sec J. 2017. № 30. P. 454–466. DOI: 10.1057/sj.2014.49.

27. Lee C.S. (2020) A crime script analysis of transnational identity fraud: Migrant offenders' use of technology in South Korea. Crime Law Soc Change. 2020. № 74. P. 201–218. DOI: 10.1007/s10611-020-09885-3.

28. Юсупов М.Ю., Путилов А.О. Фишинг как угроза конфиденциальности в сети // E-Scio. 2021. № 10(61). С. 223-232.

29. Потапкин С.Н. К вопросу о квалификации преступлений, совершаемых с использованием скимминга, по Уголовному кодексу Российской Федерации // Общество: политика, экономика, право. 2020. № 3(80). С. 30-33.

30. The National Fraud Center, Inc The growing global threat of economic and cyber crime. Available via. 2000. URL: https://www.utica.edu/academic/institutes/ecii/publications/media/global_threat_crime.pdf.

31. Goodman M. (2010) International dimensions of cybercrime. In: Ghosh S., Turrini E. (eds) Cybercrimes: A multidisciplinary analysis. 2010. P. 311–339. Springer, Heidelberg. DOI: 10.1007/978-3-642-13547-7.

32. HSN Consultants. The Nilson report. Available via. 2019. URL: https://nilsonreport.com/upload/content_promo/The_Nilson_Report_Issue_1164.pdf.m.

33. 2018 US Code. Title 18 – Crimes and Criminal Procedure. Part I – Crimes. Chapter 63 – Mail Fraud and Other Fraud Offenses. Sec. 1344 – Bank fraud. URL: https://www-fdic-gov.translate.goog/regulations/laws/rules/8000-1250.html?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=nui,sc (дата обращения: 20.11.2021).

34. Meijerink T.J. Carding: Crime prevention analysis. Available via. 2013. URL: http://purl.utwente.nl/essays/63027.